

Article

Modelling and Research on Intuitionistic Fuzzy Goal-Based Attack and Defence Game for Infrastructure Networks

Zhe Li , Jin Liu, Yibo Dong , Jiaqi Ren and Weili Li *

Science and Technology on Information Systems Engineering Laboratory, National University of Defense Technology, Changsha 410073, China; lizhe@nudt.edu.cn (Z.L.); liujin229234@nudt.edu.cn (J.L.); dongyibo@nudt.edu.cn (Y.D.); jiaqiren@nudt.edu.cn (J.R.)

* Correspondence: weiwei6563@nudt.edu.cn

Abstract: Network attack and defence games are gradually becoming a new approach through which to study the protection of infrastructure networks such as power grids and transportation networks. Uncertainty factors, such as the subjective decision preferences of attackers and defenders, are not considered in existing attack and defence game studies for infrastructure networks. In this paper, we introduce, respectively, the attacker's and defender's expectation value, rejection value, and hesitation degree of the target, as well as construct an intuitionistic fuzzy goal-based attack and defence game model for infrastructure networks that are based on the maximum connectivity slice size, which is a network performance index. The intuitionistic fuzzy two-player, zero-sum game model is converted into a linear programming problem for solving, and the results are analysed to verify the applicability and feasibility of the model proposed in this paper. Furthermore, different situations, such as single-round games and multi-round repeated games, are also considered. The experimental results show that, when attacking the network, the attacker rarely attacks the nodes with higher importance in the network, but instead pays more attention to the nodes that are not prominent in the network neutrality and median; meanwhile, the defender is more inclined to protect the more important nodes in the network to ensure the normal performance of the network.

Keywords: infrastructure networks; attack and defence games; intuitionistic fuzzy set; network science; repeated games



Citation: Li, Z.; Liu, J.; Dong, Y.; Ren, J.; Li, W. Modelling and Research on Intuitionistic Fuzzy Goal-Based Attack and Defence Game for Infrastructure Networks. *Entropy* **2023**, *25*, 1558. <https://doi.org/10.3390/e25111558>

Academic Editors: Yongchuan Tang and Deyun Zhou

Received: 19 October 2023
Revised: 15 November 2023
Accepted: 16 November 2023
Published: 18 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the continuous development of science and technology, people's daily lives are more and more inseparable from the support of various infrastructure networks. Whether it is a larger network such as the power network and aviation network, or a smaller network such as the underground line network, the paralysis of any infrastructure network will bring about immeasurable social impact and economic property losses. However, security incidents on infrastructure networks are frequent. For example, on 16 September 2022, a fire broke out in the Changsha Telecom Building, which affected the voice function of some users' mobile phones, as well as caused huge economic and property losses. While these infrastructure networks bring great convenience to people's lives, they also face great security and defence challenges, and they are more likely to become important military targets in wartime. Research points out the ever-growing importance of network resilience against targeted attack and error [1,2]. Therefore, how to respond to the attacks of terrorist organisations on infrastructure and how to make use of existing resources for effective protection are the focus of attention for the security and defence departments of various countries [3].

From the current information, most of the research on attack and defence games in infrastructure networks is now set in the context of deterministic conditions [4–6], which rely on objective indicators in complex networks for modelling [7,8], such as node degree, network efficiency, etc. In practice, however, the situation is so intricate and confusing that

it is difficult to model and predict, with certainty, the realistic conditions faced by both attackers and defenders. In addition, the huge amount of data information involved in the game, as well as the subjective decision preferences of both attackers and defenders, further increase the uncertainty of the game. Therefore, it is necessary to more comprehensively consider the ambiguities and uncertainties involved in real-world problems on the basis of the existing research on attack and defence games in infrastructure networks.

This paper introduces the membership degree and non-membership degree of intuitionistic fuzzy sets to quantitatively reflect the uncertainty of game objectives induced by the subjective decision-making preferences of players, based on the existing objective attack and defense game models. This article's game model gives more information for players' strategy choices by developing the expectation value, rejection value, and hesitation degree of the target, bringing the game model closer to reality and making decisions more sensible. When compared to existing models, the game model in this article gives more information for players' strategy choosing, bringing the game model closer to reality and making judgments more rational. Therefore, the main work and innovations of this paper are as follows:

1. Modelling offensive and defensive games from a network science perspective.
2. An intuitionistic fuzzy, goal-based game model for the attack and defence scenarios of infrastructure networks is developed.
3. Algorithms are designed to solve the developed model, and the results are analysed.
4. The repeated game process is studied.

The rest of the paper is organised as follows: Section 2 contains the literature review of this study; Section 3 provides a detailed portrayal of the game model; Section 4 gives the methodology for solving the game model; Section 5 is the experimental analysis part of the paper; and Section 6 concludes the full paper.

2. Literature Review

Realistic critical infrastructure networks often have thousands of nodes, with individual nodes interconnecting and interacting with each other to form a complex network structure. In the late 1950s, the Hungarian mathematicians Erdős and Rényi proposed the stochastic network model [9], which initiated the study of complex networks. It was not until the recent last few decades—after Watts and Strogatz proposed the small-world network model [10] and Barabási and Albert proposed the scale-free network model [11,12], that the number of studies on complex networks increased significantly. Numerous scholars have studied complex networks from the perspective of complex network models, as well as analysed the topological features of different models and their applications [13–16], which have continuously promoted the development of complex network-related research.

With the increasing threats to infrastructure networks, game theory has become a powerful research tool in infrastructure network security problems. Furthermore, many scholars have combined game theory with critical infrastructure networks, as well as constructed different complex network attack and defence game models to study the attack and protection problems of critical infrastructure networks. Borwn et al. [17] applied game theory to military strikes and homeland defence as early as 2003, and they also conducted a great deal of studies based on it. In addition, they studied a dynamic game model through two-layer and three-layer planning models, as well as analysed optimal attack strategies under the three defensive strategies of no defensive behaviour, protecting critical nodes, and protecting three-quarters of nodes [18]. Li et al. [19–21] established a two-player static game model on complex networks, as well as studied equilibrium strategies and node degrees. The relationship between equilibrium strategies and node degree values, as well as the effects of network structure, cost constraints, and cost sensitivity on the equilibrium outcome were investigated. Fu et al. [22] added a dynamic game model in which the defender first protects the network through protection or camouflage behaviours, whereby the attacker then takes measures to destroy the network. Following this, they investigated the effect of the defender's willingness on the defender

by using evolutionary games. Gu et al. [23] developed a Bayesian Stackelberg game model to analyse the effect of type distribution on an equilibrium solution in the face of the attacker having different utility functions. Jiang et al. [24] developed a Bayesian Stackelberg game model to study the water supply network protection problem, including four private information situations. Zeng et al. [25,26] focused on the problem of scheduling critical infrastructure network defence resources under conditions of asymmetric information, thereby introducing the Stackelberg active deception game and the Bayesian Stackelberg game to build the model. Zhang et al. [8] investigated the optimal allocation of resources between the defender and the attacker's multiple true/false objectives by building an asynchronous action game. Thompson et al. [27,28] developed and solved a defender–attacker–defender optimisation model to plan the optimal defence and response to intelligent attacks on the US air transport network. Yuan et al. [29] proposed to extend the traditional defender–attacker–defender model to post-incident corrective line switching operations as an effective post-incident mitigation method through which to protect the power infrastructure network. Abidi, M.H. et al. [30] proposed a vulnerability model for a CPS resource allocation process using a two-stage min-max game to minimise the value of loss costs. R. B. Benisha et al. [31] developed a two-step tracking model for UVI attacks against power grids using game theory ideas to improve detection efficiency and security. Li et al. [32] constructed an infrastructure network protection strategy solution model with “uncertain attack resources and limited protection resources”, as well as explored the effectiveness and practicality of the PSDA algorithm under conditions of incomplete information. Wang et al. [33] proposed an active defence strategy selection method for military information networks in the form of pure strategies. Jiang et al. [34] established an attack–defence two-layer game model, as well as a defence–attack–defence three-layer sequential game model for different infrastructure network attack–defence scenarios; following this, it was found that the effectiveness of the obtained defence strategies was significantly improved. As shown in Table 1, the literature review table provides a more visual display of related studies.

However, there are a large number of uncertainties in real situations that are difficult to model and to quantify effectively [35]. Moreover, the theory of intuitionistic fuzzy games provides a good idea for the solution of the above problems. In 1986, Atanassov, a Bulgarian scholar, proposed the concept of the intuitionistic fuzzy set (IFS) [36], which laid the theoretical foundation for the development of intuitionistic fuzzy games. Subsequently, Delgado defined two characteristics of fuzzy numbers [37], Angelov studied the intuitionistic fuzzy optimisation model [38], and Aggarwal gave a two-player zero-sum game solution method with the goal of the intuitionistic fuzzy set (which pushed the theory of the intuitionistic fuzzy game to maturity) [39]. In recent years, the establishment of the model in this paper is mainly based on the intuitionistic fuzzy goal zero-sum game model of Li and Nan [40,41].

Table 1. Summary of the application of game theory in the field of attack and defence game for infrastructure networks.

Game Model	Author	Research Methods
Stackelberg game model	Zeng [25,26]	Generate a pseudo network, disclose false network structure information to attackers, and use asymmetric information to actively defend against cost constraints.
	Gu [23]	Analyze the influence of different utility function types of attackers on the equilibrium solution.
	Jiang [24]	Developed a Bayesian Stackelberg game model to study the water supply network protection problem, including four private information situations.

Table 1. Cont.

Game Model	Author	Research Methods
Dynamic game model	Borwn [17]	Establish two-layer and three-layer planning models. The defender first protects the network through protection or camouflage behaviors, then the attacker takes measures to destroy it. The selection of active defense strategies is carried out in the form of pure policies.
	Fu [22]	
	Wang [33]	
Two-player zero-sum game model	Li [19–21]	Define the strategy and benefit according to the topology of the infrastructure system, and construct the benefit matrix by enumerating all the strategies to solve the problem.
Defender-attacker-defender sequential game model	Jiang [34], Thompson [27,28], Yuan [29]	The offensive and defensive process is modeled into three phases: (1) the defender invests in the infrastructure system with limited resources; (2) the attacker sees these investments and attacks the system to maximize the damage effect; (3) The defender repairs the network at the minimum cost according to the existing investment and attack to reduce losses, such as swapping edges and reducing load.
Asynchronous game model	Zhang [8]	Defenders allocate defensive resources to construct false targets to fortify real targets; Attackers allocate resources to identify false targets and attack real targets, enabling the allocation of defense resources among multiple targets.

3. Model

A complete game model is mainly composed of model assumptions, strategy sets, and payoff functions, and these aspects are mainly modelled and introduced in this section.

3.1. Symbol Definitions

The definitions and explanations of the symbols used in this paper are presented in Definitions.

3.2. Model Assumptions

The game model in this paper contains only two players—namely the attacker, that is, the player p_1 , and the defender, that is, the player p_2 . Under limited resource constraints, the offensive and defensive sides conduct offensive and defensive games around certain nodes in a complex network. Among them, the goal of the attacker is to destroy the topology of the complex network to the greatest extent by attacking some nodes in the network, thereby reducing the performance of the complex network and making it unable to maximise its effectiveness; the goal of the defender is to make the complex network work properly by protecting certain nodes in a complex network. In view of the game model in this chapter, the following assumptions are made.

1. In this game model, only one attacker and one defender are involved. And both sides have complete information, that is, they both know the complete topology of the complex network, as well as understand all the potential strategies and benefits of each other's strategies. Furthermore, the offensive and defensive sides are abso-

- lutely rational, and they can respond accordingly according to each other's actions to maximise their own interests.
2. The attack and defence are targeted at the nodes. Attackers will choose certain nodes to attack, and defenders will choose certain nodes to protect. If a node is successfully attacked, the edges connected to the node will also be removed.
 3. If a node is attacked by an attacker without the protection of the defender, it will be considered to be successfully attacked and removed from the network. However, if the node is protected by the defender, the attacker's attack on it will be deemed invalid, and the node will continue to play its role in the network.
 4. Attackers and defenders act simultaneously, that is, both sides do not know the specific strategies adopted by each other before they act. The game can be carried out in one round or multiple rounds. Specifically, the offensive and defensive sides deliver corresponding action strategies, as well as calculate the income values of the offensive and defensive sides under this strategy profile so as to obtain the income matrix. If a multi-round game is carried out, the game between the two sides will be carried out on a complex network after removing the successfully attacked nodes.
 5. The cost of an attacker attacking each node is the same and is not affected by the attributes of the node itself; similarly, the cost of defenders defending each node is the same.

3.3. Network Modeling

The complex networks studied in this game model are all unweighted and undirected graphs, which can be represented by $G = (V, E)$, where $V = [v_1, v_2, \dots, v_N]$ represents the set of all nodes, and $E \subseteq V \times V$ is the set of all edges. Let $N = |V|$ denote the number of nodes, then $A(G) = (a_{ij})_{N \times N}$ can be used to represent the adjacency matrix of the network. If there is an edge connection between the node v_i and the node v_j , then $a_{ij} = a_{ji} = 1$, otherwise, $a_{ij} = a_{ji} = 0$, which means that there is no edge connection between the node v_i and the node v_j .

3.4. Game Strategy

The network attack–defence game model studied in this paper aims at the nodes in the network; as such, the strategy set is the nodes in the network. It is assumed that the cost of both sides of the game to attack and defend each node is 1, the available resources of the attacker are n_A , and the available resources of the defender are n_D , that is, the total number of nodes that the attacker can attack at one time is n_A , and the total number of nodes that the defender can defend at one time is n_D . The vector $X_A = [x_1, x_2, \dots, x_N] \in S_A$ is defined as an attack strategy, where N is the number of nodes in a complex network, and S_A is the set of all attack strategies. If the attacker chooses to attack the i node, then $x_i = 1$, otherwise, $x_i = 0$. From this we can obtain that, for any attack strategy $\sum_{i=1}^N x_i = n_A$ holds. Similarly, the vector $Y_D = [y_1, y_2, \dots, y_N] \in S_D$ represents a defensive strategy, where S_D is a set of all defensive strategies, $y_i = 1$ and $y_i = 0$ represent the defender's choice of defensive and non-defensive i nodes, respectively, and $\sum_{i=1}^N y_i = n_D$ exists for any defensive strategy.

According to the assumption in the previous section, when the node v_i is not protected by the defender and is attacked by the attacker, it will be considered as successfully attacked and removed from the network, that is, when $x_i = 1$ and $y_i = 0$, the node v_i will be removed. As shown in Figure 1, this is a schematic diagram of the attack and defence process around the node in the attack and defence game for infrastructure networks.

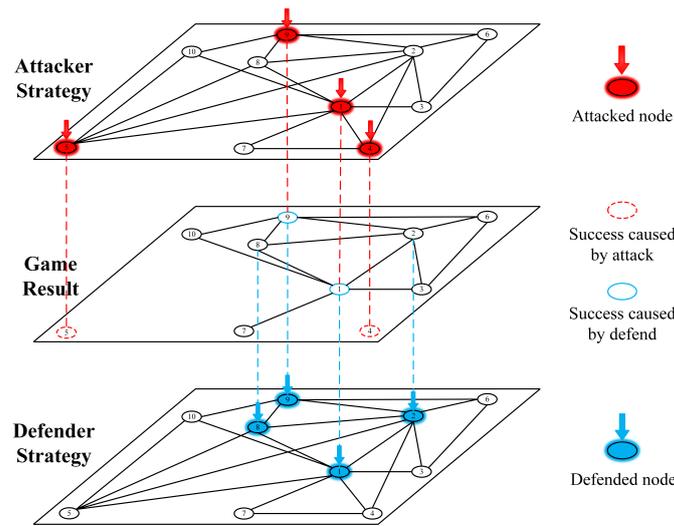


Figure 1. This figure shows the process of attack and defense game for infrastructure networks. The nodes in this picture that are covered in blue are those that the defender chooses to defend, and the nodes that are covered in red are those that the attacker decides to attack. The nodes with the red dotted line indicate that the attacker has successfully attacked them when it is not defended, and the nodes with the blue solid line indicate that the defender has successfully defended them.

After a round of a game, the set of all removed nodes is $\hat{V} \subseteq V$, the set of all remaining edges after removing nodes is $\hat{E} \subseteq (V - \hat{V}) \times (V - \hat{V})$, and the network at this time is recorded as $\hat{G} = (V - \hat{V}, \hat{E})$. Thus, \hat{V} can be obtained by the following equation:

$$\hat{V} = V^A - V^A \cap V^D \tag{1}$$

Among them, $V^A \subseteq V$ is the set of all the attack nodes; $V^D \subseteq V$ is the set of all the defensive nodes.

3.5. Payoff Function

The payoff function is used to calculate the payoff of the offensive and defensive sides under different strategic profiles. In this chapter, we define the payoff function of both sides based on the network performance evaluation function. The network performance evaluation function can reflect the overall topology of the network and reflect the impact of different node deletions on the performance of the entire network. Generally, the maximum connected slice size, the number of reachable node pairs, and the network efficiency are used to evaluate the network performance. Furthermore, $U^A(X_A, Y_D)$ is defined as the attacker’s payoff function, where X_A is the attack strategy selected by the attacker, and Y_D is the defensive strategy selected by the defender. The calculation formula is as follows:

$$U^A(X_A, Y_D) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0, 1] \tag{2}$$

Similarly, $U^D(X_A, Y_D)$ is defined as the defender’s payoff function, which is computed as follows:

$$U^D(X_A, Y_D) = \frac{\Gamma(\hat{G}) - \Gamma(G)}{\Gamma(G)} \in [-1, 0] \tag{3}$$

Among them, Γ is the network performance evaluation function, which does not increase monotonously with the decrease in the number of network nodes. Thus, the complex network \hat{G} after the nodes are removed is a subgraph of the original complex network G , which means $\Gamma(\hat{G}) \leq \Gamma(G)$. This attribute indicates that the network’s performance suffers when nodes are removed.

This chapter selects the maximum connected slice size as an indicator to evaluate the network performance. The maximum connected slice size in a complex network refers to the number of nodes contained in the greatest connected subgraph, which determines the network’s reachability and information transmission efficiency. If there are several disconnected subgraphs in the network, there is no information exchange between them, and the network’s goals cannot be met. As a result, the maximum connectivity slice size can be utilized to assess the network’s connection and information transmission efficiency. The following formula can be used to calculate the maximum connected slice size:

$$L_{max} = \max_{i=1}^n |C_i| \tag{4}$$

Among them, n represents the total number of nodes in the complex network, C_i represents the connected subgraph where node i is located, and $|C_i|$ indicates the number of nodes in the subgraph.

4. Methods

In order to better describe the uncertainty in the game process and to make the network attack and defence game model more in line with the actual situation, the game model used in this chapter is an intuitionistic fuzzy target, zero-sum game model, and the solution method will be introduced below. According to the research of Nan and Li on the intuitionistic fuzzy goal zero-sum game model [40], we define our intuitionistic fuzzy goal zero-sum game model as the following multivariate array:

$$IFG = (X, Y, F, v_a, p_a, v_r, p_r, \omega_a, q_a, \omega_r, q_r) \tag{5}$$

Here, X and Y are the mixed strategy spaces of player p_1 and player p_2 , respectively, and this is denoted by the following:

$$X = \left\{ x \in R^m \mid \sum_{i=1}^m x_i = 1, x_i \geq 0, i = 1, 2, \dots, m \right\} \tag{6}$$

and

$$Y = \left\{ y \in R^n \mid \sum_{j=1}^n y_j = 1, y_j \geq 0, j = 1, 2, \dots, n \right\} \tag{7}$$

where the payoff matrix for player p_1 is concisely expressed as the matrix $F = (b_{ij})_{m \times n}$, and the payoff matrix for player p_2 is $-F = (-b_{ij})_{m \times n}$ since the matrix game is zero-sum. Among them, v_a is the expected value of the player p_1 to the target, and the error is $p_a \geq 0$; in addition, v_r is the rejection value of the player p_1 to the target, and the error is $p_r \geq 0$. Similarly, ω_a and ω_r represent the expected value and rejection value of the player p_2 to the target, respectively, and $q_a \geq 0$ and $q_r \geq 0$ are the corresponding errors, respectively.

Let $D = \{x^T F y \mid (x, y) \in X \times Y\} \subseteq R$ be an intuitionistic fuzzy set on D , where the payoff goal of p_1 is $A = \{\langle x^T F y, \mu_A(x^T F y), v_A(x^T F y) \rangle \mid x^T F y \in D\}$. Among these, we can express them as follows:

$$\mu_A : D \rightarrow [0, 1] \tag{8}$$

$$x^T F y \in D \quad \mu_A(x^T F y) \in [0, 1]$$

and

$$v_A : D \rightarrow [0, 1] \tag{9}$$

$$x^T F y \in D \quad v_A(x^T F y) \in [0, 1]$$

and satisfy

$$0 \leq \mu_A(x^T F y) + v_A(x^T F y) \leq 1 \tag{10}$$

Similarly, for the player p_2 , its goal on the payoff value is also an intuitionistic fuzzy set on D , which is in the form of $B = \{ \langle x^T Fy, \mu_B(x^T Fy), v_B(x^T Fy) \rangle \mid x^T Fy \in D \}$. Among these, we can express them as follows:

$$\begin{aligned} \mu_B : D &\rightarrow [0, 1] \\ x^T Fy \in D \quad \mu_B(x^T Fy) &\in [0, 1] \end{aligned} \tag{11}$$

and

$$\begin{aligned} v_B : D &\rightarrow [0, 1] \\ x^T Fy \in D \quad v_B(x^T Fy) &\in [0, 1] \end{aligned} \tag{12}$$

and satisfy

$$0 \leq \mu_B(x^T Fy) + v_B(x^T Fy) \leq 1 \tag{13}$$

Among them, the membership degree $\mu_A(x^T Fy)$ is the acceptance degree of the player p_1 to the payment value, and the non-membership degree $v_A(x^T Fy)$ is the rejection degree of the player p_1 to the payment value; similarly, the membership degree $\mu_B(x^T Fy)$ and the non-membership degree $v_B(x^T Fy)$ represent the degree of acceptance and rejection of the payoff value by the player p_2 , respectively.

It is assumed that the membership function and non-membership function of the player p_1 are linear as follows:

$$\mu_A(x^T Fy) = \begin{cases} 0 & (x^T Fy < v_a - p_a) \\ 1 - (v_a - x^T Fy) / p_a & (v_a - p_a \leq x^T Fy < v_a) \\ 1 & (x^T Fy \geq v_a) \end{cases} \tag{14}$$

$$v_A(x^T Fy) = \begin{cases} 1 & (x^T Fy < v_r - p_r) \\ (v_r - x^T Fy) / p_r & (v_r - p_r \leq x^T Fy < v_r) \\ 0 & (x^T Fy \geq v_r) \end{cases} \tag{15}$$

A schematic diagram of the membership function and non-membership function of the player p_1 is shown in Figure 2.

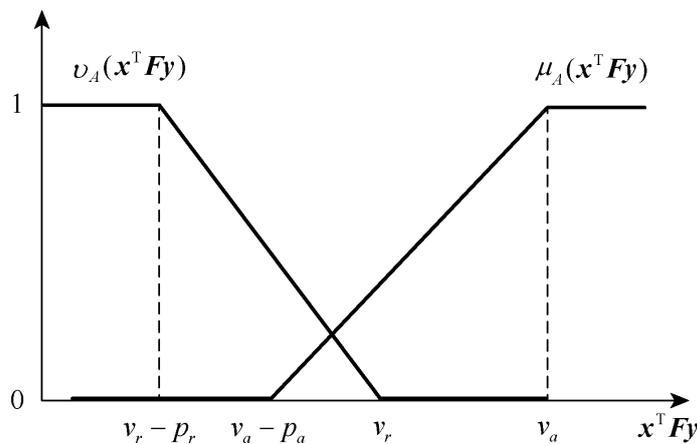


Figure 2. This figure shows the membership function and non-membership function image of player p_1 . And the membership function monotonically non-decreasing as the payment value increases; While the non-membership function monotonically non-increasing as the payment value increases.

From the function image, we can obtain that, when $x^T Fy \leq v_r - p_r$, the satisfaction degree of the player p_1 is 0, and the rejection degree is 1; when $v_r - p_r < x^T Fy \leq v_a - p_a$,

then the satisfaction degree of the player p_1 is 0, but because the player p_1 has a certain degree of hesitation, it will not completely refuse at this time; when $v_r < x^T Fy \leq v_a$, then the degree of rejection of the player p_1 is reduced to 0, but because the player p_1 has a certain degree of hesitation, it will not be fully satisfied at this time; and when $x^T Fy > v_a$, then the satisfaction degree of the player p_1 is 1, and the rejection degree is 0. It can be seen that the intuitionistic fuzzy set reflects the degree of satisfaction, rejection, and hesitation of the player p_1 for the target in all aspects, and it can fully characterise the fuzziness and uncertainty in the real game problem.

Similarly, the membership function and non-membership function of the player p_2 are also linear.

$$\mu_B(x^T Fy) = \begin{cases} 1 & (x^T Fy < \omega_a) \\ 1 - (x^T Fy - \omega_a) / q_a & (\omega_a \leq x^T Fy < \omega_a + q_a) \\ 0 & (x^T Fy \geq \omega_a + q_a) \end{cases} \quad (16)$$

$$v_B(x^T Fy) = \begin{cases} 0 & (x^T Fy < \omega_r) \\ (x^T Fy - \omega_r) / q_r & (\omega_r \leq x^T Fy < \omega_r + q_r) \\ 1 & (x^T Fy \geq \omega_r + q_r) \end{cases} \quad (17)$$

A schematic diagram of the membership function and non-membership function of the player p_2 is shown in Figure 3. According to the image, it can also be interpreted similarly to the player p_1 .

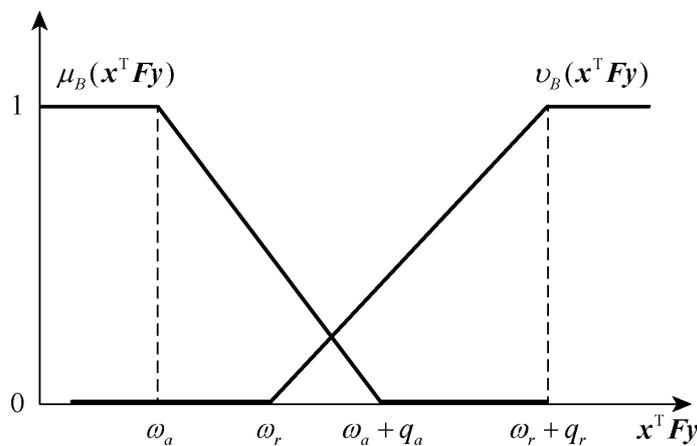


Figure 3. This figure shows the membership function and non-membership function image of player p_2 . And the membership function monotonically non-increasing as the payment value increases; While the non-membership function monotonically non-decreasing as the payment value increases.

In the two-person zero-sum game, a gain for one player means a loss for the other. For the players p_1 and p_2 , both sides want to maximise their own benefits and minimise their own losses. Since the membership function and non-membership function of player p_1 are both linear functions, the maximum-minimum strategy x^* of player p_1 can be obtained by solving the following linear programming problem.

$$\begin{aligned} & \max\{\alpha - \beta\} \\ & \text{s.t.} \left\{ \begin{array}{l} \sum_{i=1}^m a_{ij}x_i + p_a - v_a \geq p_a\alpha \quad (j = 1, 2, \dots, n) \\ \sum_{i=1}^m a_{ij}x_i - v_r \geq -p_r\beta \quad (j = 1, 2, \dots, n) \\ x_1 + x_2 + L + x_m = 1 \\ x_i \geq 0 (i = 1, 2, \dots, m) \\ 0 \leq \alpha \leq 1, 0 \leq \beta \leq 1 \\ \alpha + \beta \leq 1 \end{array} \right. \end{aligned} \tag{18}$$

Among them, α, β, x_i ($i = 1, 2, \dots, m$) are decision variables.

Similarly, the membership function and non-membership function of player p_2 are also linear functions, thus the minimum-maximum strategy y^* of player p_2 can be obtained by solving the following linear programming problem.

$$\begin{aligned} & \min\{\eta - \lambda\} \\ & \text{s.t.} \left\{ \begin{array}{l} \sum_{j=1}^n a_{ij}y_j - \omega_a - q_a \leq -q_a\lambda \quad (i = 1, 2, \dots, m) \\ \sum_{j=1}^n a_{ij}y_j - \omega_r \leq q_r\eta \quad (i = 1, 2, \dots, m) \\ y_1 + y_2 + L + y_n = 1 \\ y_j \geq 0 (j = 1, 2, \dots, n) \\ 0 \leq \lambda \leq 1, 0 \leq \eta \leq 1 \\ \lambda + \eta \leq 1 \end{array} \right. \end{aligned} \tag{19}$$

Among them, η, λ, y_i ($i = 1, 2, \dots, n$) are decision variables.

By solving the above two linear programming problems, the mixed strategy Nash equilibrium of the game model can be obtained.

5. Results

In this paper, the experiments use the following environment configuration: GPU model NVIDIA GeForce RTX 3060, 2.3 GHz CPU and 64 GB RAM.

5.1. Infrastructure Network Model Example

In this paper, the target infrastructure network shown in Figure 4 is used. The target network contains 16 nodes and 27 edges, of which the maximum degree of node 6 is 7, and the minimum degree of nodes 8, 12, 15, and 16 is 1. This target infrastructure network is a model of real-world infrastructure network topologies such high-speed rail networks, airport networks, and power transmission networks. Using the high-speed railway network as an example, the nodes in the complex network topology diagram represent different stations in the high-speed railway network, and the connecting edges between the nodes indicate the lines that trains travel between. In the actual world, if a station is attacked and compromised, and its train transfer function is lost, all lines that pass through the station are disabled.

In this chapter, we use the maximum connected patch size as the network performance evaluation function Γ , and we stipulate that the resources available to the attacker and the defender are equal, both of which are 4—that is, $n_A = n_D = 4$.

5.2. Results of Single Attack and Defense Game

The experimental steps of this section are as follows :

1. Generate adjacency matrix. According to the topological structure diagram of the target network, the corresponding adjacency matrix $A(G) = (a_{ij})_{N \times N}$ is calculated. If there is an edge connection between the node v_i and the node v_j , then $a_{ij} = a_{ji} = 1$, otherwise, $a_{ij} = a_{ji} = 0$.
2. Generate a revenue matrix. The attacker gives an attack strategy, and the defender gives a defence strategy. Such a combination of attack and defence strategies constitutes a strategy profile. By traversing all strategy combinations, the gains of attackers and defenders under different strategy profiles are calculated, and finally the gain matrix is obtained.
3. Solve the mixed strategy Nash equilibrium. Based on the solution method in the previous section, we set the attacker's expectation value v_a for the target, and the corresponding error p_a ; furthermore, the attacker's rejection value of the target v_r corresponds to the error p_r . Set the defender's expectations of the target value w_a and the corresponding error q_a ; moreover, the defender's rejection of the target value w_r correspond to the error q_r . By calling the MATLAB linear programming solver, the mixed strategy Nash equilibrium is obtained.

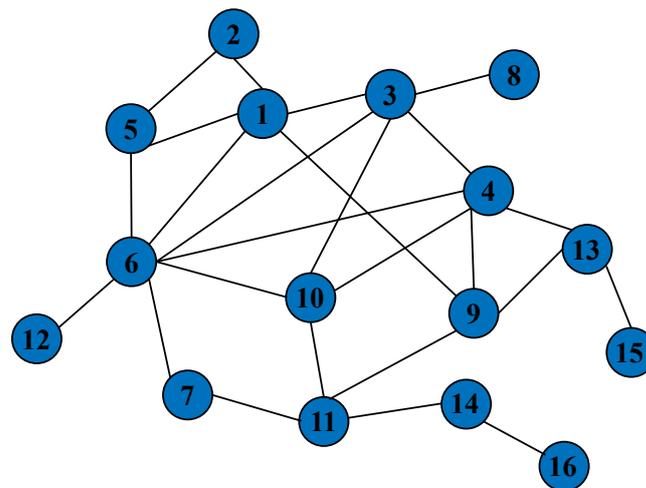


Figure 4. This figure shows the topology of the target infrastructure network. Nodes represent stations with specialized purposes in real-world complex networks, such as high-speed train stations, airports, and power stations; A linked edge is defined as a physical or logical connection between two nodes that allows them to exchange information or matter.

In this experiment, we stipulated that the resources available to the attacker and the defender are equal, that is $n_A = n_D = 4$, which means the attacker can only attack 4 nodes at a time, and the defender can only defend 4 nodes at a time. Thus, the attacker's policy set contains a total of $C_{16}^4 = 1820$ policies; similarly, the defender's strategy set contains a total of $C_{16}^4 = 1820$ strategies, and the number of strategy profiles reaches 3, 312,400. By traversing these policy profiles, the payoff function is used to calculate the payoff of attackers and defenders under different policy profiles, and the corresponding payoff matrix is obtained.

According to the payoff matrix, we set the attacker's expectation of the target $v_a = 0.4$, which corresponds to the error $p_a = 0.3$; furthermore, the attacker's rejection value of the target is $v_r = 0.25$, which corresponds to the error $p_r = 0.2$. That is, when the attack strategy reduces the performance of the target network by less than 5%, the attacker's satisfaction

degree is 0, and the rejection degree is 1; when the attack strategy reduces the performance of the target network by 5 ~10%, the attacker’s satisfaction is 0, but because the attacker has a certain degree of hesitation, it will not be completely rejected at this time; when the attack strategy reduces the performance of the target network by 25 ~40%, the attacker’s rejection degree is reduced to 0, but because the attacker has a certain degree of hesitation, it is not completely satisfied at this time; and when the attack strategy reduces the performance of the target network by more than 40%, the attacker’s satisfaction degree is 1 and the rejection degree is 0. The image of the attacker’s membership and non-membership functions is shown in Figure 5.

Set the defender’s expectations of the target value $w_a = 0.1$, and the corresponding error is $q_a = 0.2$; the defender’s rejection of the target value is $w_r = 0.15$, which corresponds to the error $q_r = 0.25$. The specific explanation is similar to the attacker. The membership function and non-membership function images of the defender are shown in Figure 6.

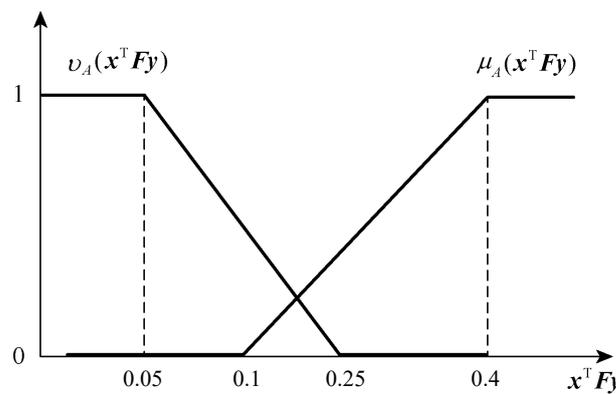


Figure 5. This figure shows the image of the attacker’s membership function and non-membership function. And the image of attacker’s membership and non-membership function are obtained with $v_a = 0.4, p_a = 0.3, v_r = 0.25, p_r = 0.2$.

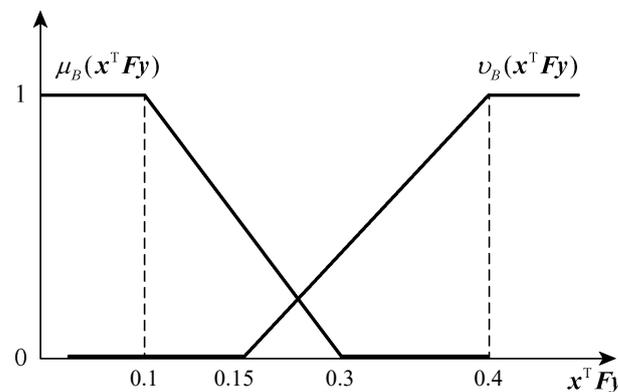


Figure 6. This figure shows the image of the defender’s membership function and non-membership function. And the image of defender’s membership and non-membership function are obtained with $w_a = 0.1, q_a = 0.2, w_r = 0.15, q_r = 0.25$.

The MATLAB linear programming solver was called, and the results of the mixed strategy Nash equilibrium are shown in Table 2. The pure strategy with a probability that was not equal to 0 in an equilibrium state and its corresponding equilibrium probability are given in the table. It can be seen from the equilibrium results that the attacker had 11 pure strategies with a probability greater than 0 to choose from, among which the probability assigned to { 3, 6, 13, and 14 } was the highest, and the degree of the remaining nodes was not prominent except for 6 nodes. The defender had 10 pure strategies with a probability greater than 0 to choose from, among which the probability assigned to { 1, 3, 9, and 11 } was the highest, and the degree of these four nodes was more prominent.

Table 2. Mixed strategy probability distribution table under equilibrium state.

Attack Strategy	Probability	Defence Strategy	Probability
{ 1, 3, 5, 14 }	0.0104	{1, 3, 6, 9 }	0.1077
{ 1, 4, 6, 11 }	0.0414	{ 1, 3, 9, 11 }	0.2500
{ 1, 4, 7, 10 }	0.0473	{ 1, 6, 9, 13 }	0.0828
{ 1, 5, 6, 11 }	0.0518	{ 1, 6, 13, 14 }	0.0594
{ 1, 5, 12, 14 }	0.1760	{ 3, 4, 6, 14 }	0.0947
{ 1, 6, 13, 14 }	0.0207	{ 3, 10, 11, 14 }	0.0476
{ 3, 5, 6, 11 }	0.0104	{ 6, 9, 13, 14 }	0.0361
{ 3, 6, 11, 13 }	0.0207	{ 6, 10, 11, 13 }	0.1238
{ 3, 6, 13, 14 }	0.2899	{ 9, 11, 13, 14 }	0.1297
{ 3, 11, 12, 13 }	0.1657	{ 10, 11, 13, 14 }	0.0727
{ 4, 7, 9, 10 }	0.1657		

When the attacker chooses the hybrid Nash equilibrium strategy, the minimum degree of reaching the expected goal is 0.5268, the maximum degree of reaching the rejection goal is 0, and the degree of hesitation is 0.4732. When the defender chooses the mixed strategy Nash equilibrium, the minimum degree of reaching the expected goal is 0.4322, the maximum degree of reaching the rejection goal is 0.2098, and the degree of hesitation is 0.3580.

In order to further explore the preferences of attackers and defenders to attack and defend nodes, we mapped the mixed strategy probability distribution to nodes as shown in Equations (19) and (20) as follows:

$$\rho_A = \frac{1}{n_A} \sum_{i=1}^{|S_A|} p_i \cdot X_i = \frac{1}{n_A} \sigma_A \cdot X_{|S_A| \times N} \tag{20}$$

$$\rho_D = \frac{1}{n_D} \sum_{j=1}^{|S_D|} q_j \cdot Y_j = \frac{1}{n_D} \sigma_D \cdot Y_{|S_D| \times N} \tag{21}$$

Among them, $\rho_A = [\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_i, \dots, \tilde{p}_N]$ represents the probability that the attacker allocates to each node in the Nash equilibrium, and $\rho_D = [\tilde{q}_1, \tilde{q}_2, \dots, \tilde{q}_j, \dots, \tilde{q}_N]$ represents the probability the defender allocates to each node in the Nash equilibrium. $\sigma_A = [p_1, p_2, \dots, p_i, \dots, p_{|S_A|}]$ and $\sigma_D = [q_1, q_2, \dots, q_j, \dots, q_{|S_D|}]$ denote the probability distribution of all pure strategies in the Nash equilibrium.

The probability distribution of the equilibrium results mapped to different nodes in Table 2 is shown in Table 3. From Table 3, it can be seen that attackers pay high attention to nodes 1, 3, 6, 12, 13, and 14, while the degree and betweenness of nodes 1, 3, 13, and 14 are at a medium level. In addition, nodes 12, and even edge nodes, indicated that, when attacking the network, the attackers rarely attacked nodes with high importance in the network, but rather paid more attention to the nodes at a medium level and betweenness in the network. The attackers improved their success rate and the revenue of their attacks through such attack strategies. On the other hand, the defenders had the highest probability of defending node 11, which had the largest betweenness and highest degree in the network, thereby indicating that defenders are more inclined to protect the more important nodes in the network to ensure the normal performance of the network. In addition, the betweenness of nodes 2, 8, 15, and 16 was 0, and the probability that the attacker and the defender chose the node was also 0, thus indicating that these nodes were not of concern by both sides.

Table 3. Probability distribution tables on different nodes.

Node	1	2	3	4	5	6	7	8
Degree	5	2	5	5	3	7	2	1
Betweenness	16.9	0	14.5	14.5	2.1	29.5	4	0
Attack probability	0.087	0	0.124	0.064	0.062	0.109	0.053	0
Defence probability	0.125	0	0.125	0.024	0	0.125	0	0
Node	9	10	11	12	13	14	15	16
Degree	4	4	4	1	3	2	1	1
Betweenness	21.1	11.5	29	0	14	14	0	0
Attack probability	0.041	0.053	0.073	0.085	0.124	0.124	0	0
Defence probability	0.151	0.061	0.156	0	0.125	0.109	0	0

The probability diagrams of different nodes being attacked or defended in the equilibrium state are respectively shown in Figure 7.

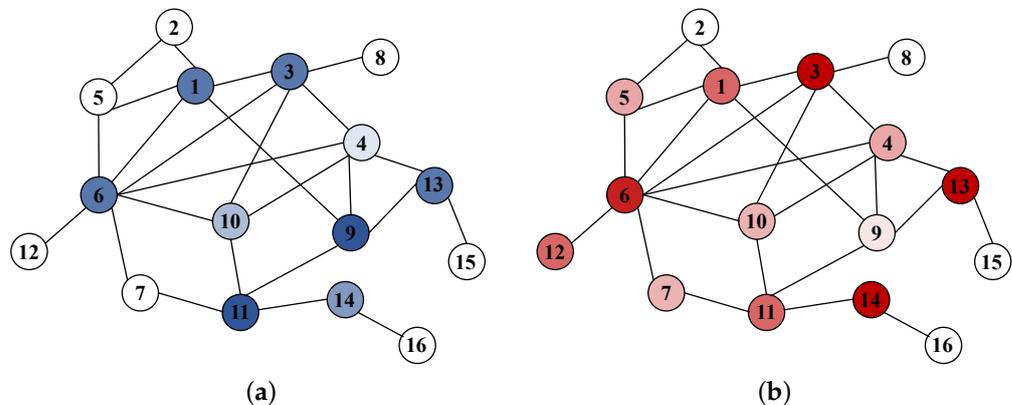


Figure 7. This picture shows the probability of different nodes being attacked or defended. The darker the colour is, the greater the probability that the node is attacked or defended. And a node with no color indicates that it is not selected by attackers or defenders. (a) The probability of different nodes being defended. (b) The probability of different nodes being attacked.

In order to verify the effectiveness of the game model in obtaining the equilibrium strategy, we selected the maximum degree strategy, the minimum degree strategy, and the random strategy to compare with the equilibrium strategy. The maximum degree strategy refers to the attack and defence of the largest nodes in the network. In contrast, if the offensive and defensive sides attack and defend the smallest nodes in the network, then this represents the minimum degree strategy; the random strategy means that the attacker and the defender do not consider the indicators of the nodes and randomly select several nodes in the network to attack and defend. Table 4 shows the gains of attackers when attackers and defenders adopt four different respective strategies. Due to the great uncertainty of the selection of random strategies, we conducted 3000 independent experiments and used the average of the final results as the final equilibrium result.

Table 4. Table of equilibrium gains for the attacker under four different strategies.

Attack	Defense			
	Nash	Max	Min	Random
Nash	0.2580	0.2836	0.5072	0.3541
Max	0.2441	0	0.5	0.3495
Min	0.25	0.25	0	0.1871
Random	0.2266	0.2358	0.2939	0.2562

We calculated the Nash equilibrium again for the equilibrium income matrix that was obtained in Table 3, and the results were $([1, 0, 0, 0], [1, 0, 0, 0])$, that is, (equilibrium strategy, equilibrium strategy) was the Nash equilibrium point. Further, both the offensive and defensive sides chose the equilibrium strategy to obtain the maximum income, which further verifies the effectiveness of the equilibrium strategy that was obtained in this section.

5.3. Results of Repeated Network Attack and Defense Game

In the previous section, we only studied the situation of one round in a game. In reality, the offensive and defensive sides will carry out multiple rounds of attack and defence around complex networks such as traffic networks and communication networks. The end state of each round of game will become the starting state of the next round of the game. Therefore, in order to be closer to the reality, we will repeat the game around the target network in this section.

In the repeated game model, we will add the following assumptions: (1) At the beginning of each round of a game, the strategy choice of the attacker and the defender is only related to the topology of the complex network in the current state, and it is not affected by the strategy choice of the two sides in the previous round of the game—that is, the repeated game has a Markov property. (2) The starting state of each round of the game is the current complex network model, and the ending state is the complex network model after deleting the successfully attacked nodes. Moreover, the ending state of that round of the game is the starting state of the next round of the game. (3) The termination condition of the repeated game is as follows: no matter what attack strategy the attacker adopts, the repeated game terminates when the node in the target network cannot be successfully attacked.

The remaining assumptions are the same.

Based on the above assumptions, the design of repeated game experiment steps was as follows:

1. Calculate the adjacency matrix.
2. Generate the income matrix
3. Solve for the mixed strategy Nash equilibrium based on the equilibrium payoff matrix.
4. Solving for mixed strategy Nash equilibrium based on the equilibrium payoff matrix.
5. Based on the mixed-strategy Nash equilibrium result, the attacker and the defender each select a pure strategy to play. We adopted a “roulette” approach for selecting pure strategies from among the equilibrium strategies.
6. Obtain the number of nodes that were successfully attacked and calculate the value of the attacker’s gain in this game. The defender’s gain is the negative of the attacker’s gain.
7. Update the complex network diagrams.

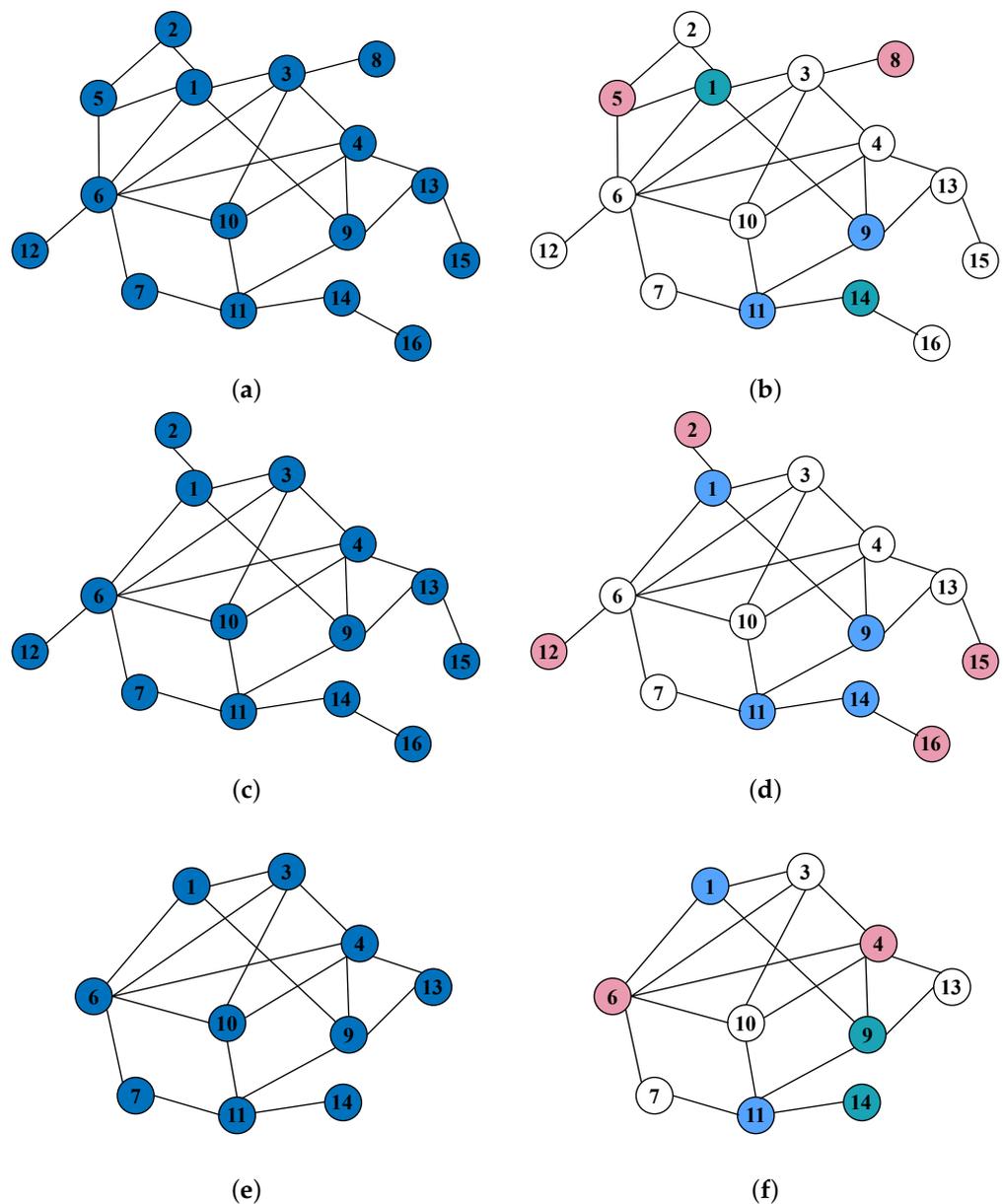
After modelling and solving, this repeated game was played 5 times to reach the termination state, and the progress of the repeated game is shown in Figure 8. For ease of record keeping, we used Max, Min, Random and Nash to represent the maximum degree strategy, minimum degree strategy, random strategy, and equilibrium strategy, respectively. The attacker’s strategy choice for each round of the game was Nash → Min → Nash → Nash → Nash; the defender’s strategy choice for each round of the game was Nash → Nash → Nash → Nash → Nash.

In the repeated game process, we found that the attacker chose the minimum degree strategy in the second round of the game, and that the gain was higher than that of the equilibrium strategy. That is to say, although the equilibrium strategy will bring more robust benefits, the equilibrium strategy is not the optimal choice in certain cases. For the defender, he has always chosen the equilibrium strategy in the repeated game process, thereby indicating that, although other strategies may bring higher earnings, the defender cannot bear the risks brought by other strategies.

The actual income in each round of the game and the equilibrium income in the current state are given in Figure 9. We find that the actual earnings of each round of the game was

not the same as the equilibrium earnings in the current state. This is because we used the 'roulette' method to select the pure strategy from the equilibrium strategy, which results in a great deal of randomness.

Now, we assume that, if the attacker knows the defender's defence strategy before choosing the attack strategy every time, then the attacker will perfectly avoid the defender's choice of the defender's node every time they choose the attack node. Under this assumption, the attacker only needs to carry out three rounds of attacks to achieve the termination condition of the repeated game. However, in the experiment of this section, the attacker carried out a total of five rounds of attacks to terminate the repeated game. The target network used in this paper only contains 16 nodes. However, the scale of complex networks in reality is huge. Repeated games on such networks may take thousands of rounds to reach the termination condition. It is of great practical significance to study the convergence of this problem and how to reach the termination condition of repeated games more quickly.



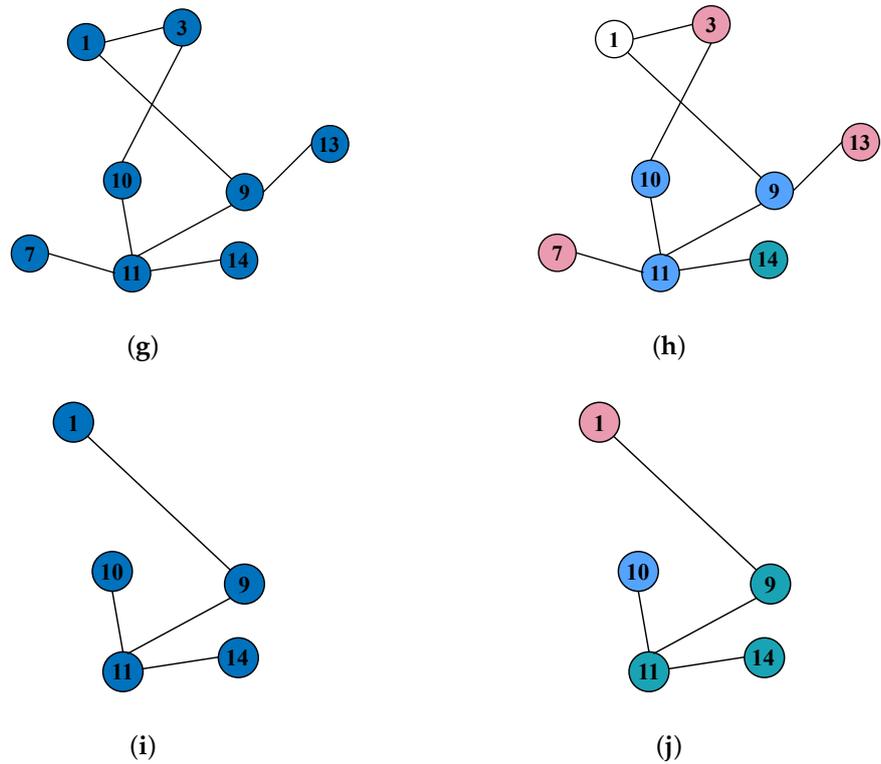


Figure 8. This picture shows the specific process of each round of a game in the process of a repeated game. Among them, the picture of the left column represents the topology of the infrastructure network at the beginning of each round of the attack and defence game. The picture in the right column shows the strategy choice of each round of attackers and defenders. The marked red node represents the node that successfully attacked, the green node represents the node that successfully defended, and the blue node represents the node that was defended but not attacked. (a) Topology of the first round of the complex network. (b) The first round of attack and defence strategy. (c) Topology of the second round of the complex network. (d) The second round of attack and defence strategy. (e) Topology of the third round of the complex network. (f) The third round of attack and defence strategy. (g) Topology of the fourth round of the complex network. (h) The fourth round of attack and defence strategy. (i) Topology of the fifth round of the complex network. (j) The fifth round of attack and defence strategy.

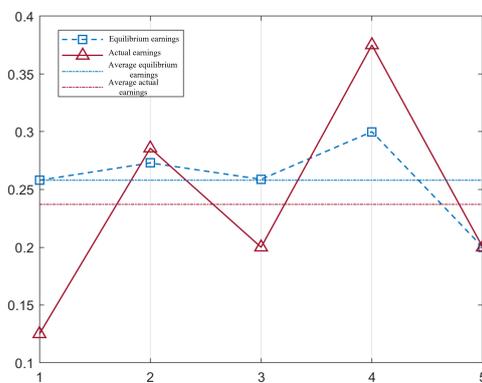


Figure 9. This figure shows the comparison between the actual earnings and the equilibrium earnings under the repeated game. The theoretical equilibrium and actual earnings of each game are shown by the blue box and red triangle nodes. And the blue dotted and red dotted lines represent the average equilibrium earnings and the average actual earnings.

6. Discussion

It is difficult for players to accurately assess the game aim in the game process due to the availability of complicated components such as information, knowledge, and subjective consciousness of the players involved in the real game. As a result, the player's impression of the game goal is ambiguous. It is precisely because of this uncertainty that the players would be hesitant about the degree of achievement of the game aim. The intuitionistic fuzzy set can be used to represent the degree to which the player accomplishes the predetermined goal and the degree of hesitancy to achieve the predetermined goal while picking the strategy, which gives the players more information to choose their strategy.

The model established by this method not only considers objective conditions such as network topology and payoff function when solving the equilibrium strategy, but it also quantitatively analyzes and evaluates subjective factors such as decision-makers' preferences and hesitation. Simultaneously, this paper for the first time introduces the two-player zero-sum game model with the goal of intuitionistic fuzzy set into the complex network attack and defense game, broadening the boundary of research on the attack and defense game of infrastructure network and providing a new research idea for solving the uncertainty problem of quantitative analysis in the field of attack and defense game of infrastructure network. Therefore, the model established in this paper has good theoretical and practical significance.

However, in the course of creating the model, this study adds additional model assumptions and strongly limits the model's field of use. In reality, obtaining the complete information required in this paper is impossible, and typically, the defender has a complete understanding of the network topology information, whereas the attacker has only limited information, which also contains false information intentionally created by the defender. Furthermore, because the importance and scale of nodes in the critical infrastructure network vary, the defender's investment cost for each node varies, as does the attacker's cost of assaulting each node. Furthermore, both defense and attack have a success rate, which ignores the reality that the node can still perform part of its duties after being attacked. Finally, this model does not work with several participants. This will become new study directions in the field of infrastructure network attack and defense games.

7. Conclusions

In this paper, a two-person, zero-sum game model, with the goal of intuitionistic fuzzy sets, was introduced into the research on complex network attack–defence games. In order to simplify the problem, we make basic assumptions in the model, as well as conduct modelling and research on the basis of assumptions. We found that, when attacking the network, attackers rarely attack the nodes with high importance in the network; instead, they pay more attention to the nodes with moderate importance and betweenness in the network, whereas defenders are more inclined to protect the more important nodes in the network to ensure the normal performance of the network. After this finding, we compared the obtained equilibrium strategy with three typical strategies, and we found that both offensive and defensive sides chose the equilibrium strategy to obtain the maximum benefit, which further verifies the effectiveness of the equilibrium strategy obtained in this paper. Finally, we conducted a repeated game modelling to simulate the actual situation in reality, and we found that, for attackers (although the equilibrium strategy will bring more robust benefits), the equilibrium strategy was not the optimal choice in certain cases; for defenders, although other strategies may bring higher earnings, the defender could not bear the risks brought by other strategies. The game model in this paper provides a new research framework and ideas for later network attack and defence game modelling. The paper concludes by discussing the theoretical and practical significance of the proposed model, as well as its application scope.

Author Contributions: Conceptualization, Z.L., J.L. and Y.D.; methodology, Z.L. and W.L.; software, Z.L.; validation, Z.L.; formal analysis, Z.L. and J.R.; investigation, J.L. and W.L.; writing, original

draft preparation, Z.L. and J.R.; writing, review and editing, Z.L., J.L. and W.L.; visualization, Z.L. and J.R.; project administration, Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to some privacy reasons.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Definitions

Symbols	Definitions
p_1, p_2	Two players in the game model
G	Scale-free network
V	Set of all nodes
E	Set of all edges
$ C_i $	Number of nodes in the subgraph
X_A	An attack strategy
Y_D	An defensive strategy
S_A	Set of all attack strategies
S_D	Set of all defensive strategies
n_A, n_D	Available resources of the player p_1 and player p_2
$U^A(X, Y), U^D(X, Y)$	Payoff function of the player p_1 and player p_2
$\Gamma(G)$	Network performance evaluation function
IFG	Intuitionistic fuzzy goal zero-sum game model
X, Y	Mixed strategy spaces of player p_1 and player p_2
v_a, v_r	Expected value and rejection value of player p_1
ω_a, ω_r	Expected value and rejection value of player p_2
p_a, p_r, q_a, q_r	Corresponding errors
$\mu_A(x^T Fy), v_A(x^T Fy)$	Membership degree and non-membership degree of player p_1
$\mu_B(x^T Fy), v_B(x^T Fy)$	Membership degree and non-membership degree of player p_2

References

- Perc, M. Evolution of cooperation on scale-free networks subject to error and attack. *New J. Phys.* **2009**, *11*, 033027. [\[CrossRef\]](#)
- Ji, P.; Ye, J.; Mu, Y.; Lin, W.; Tian, Y.; Hens, C.; Perc, M.; Tang, Y.; Sun, J.; Kurths, J. Signal propagation in complex networks. *Phys. Rep.* **2023**, *1017*, 1–96. [\[CrossRef\]](#)
- Li, Y.P. Modelling and Analysis of Attacker–defender Game in Complex Networks. Master’s Thesis, National University of Defense Technology, Changsha, China, 2018.
- Chen, J.; Touati, C.; Zhu, Q. A Dynamic Game Approach to Designing Secure Interdependent IoT-Enabled Infrastructure Network. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2601–2612. [\[CrossRef\]](#)
- Wang, S.; Sun, J.; Zhang, J.; Dong, Q.; Gu, X.; Chen, C. Attack-Defense game analysis of critical infrastructure network based on Cournot model with fixed operating nodes. *Int. J. Crit. Infrastruct. Prot.* **2023**, *40*, 100583. [\[CrossRef\]](#)
- Li, Q.; Li, M.; Gan, J.; Guo, C. A game-theoretic approach for the location of terror response facilities with both disruption risk and hidden information. *Int. Trans. Oper. Res.* **2021**, *28*, 1864–1889. [\[CrossRef\]](#)
- Feng, Q.; Cai, H.; Chen, Z. Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 105900. [\[CrossRef\]](#)
- Zhang, X.; Ding, S.; Ge, B.; Xia, B.; Pedrycz, W. Resource allocation among multiple targets for a defender-attacker game with false targets consideration. *Reliab. Eng. Syst. Saf.* **2021**, *211*, 107617. [\[CrossRef\]](#)
- Erdős, P.; Rényi, A. On random graphs. *Publ. Math.* **1959**, *6*, 290–297. [\[CrossRef\]](#)

10. Watts, D.J.; Strogatz, S.H. Collective dynamics of ‘small-world’ networks. *Nature* **1998**, *393*, 440–442. [[CrossRef](#)]
11. Barabási, A.L.; Albert, R. Emergence of Scaling in Random Networks. *Science* **1999**, *286*, 509–512. [[CrossRef](#)] [[PubMed](#)]
12. Barabási, A.L. Scale-Free Networks: A Decade and Beyond. *Science* **2009**, *325*, 412–413. [[CrossRef](#)]
13. D’Souza, R.M.; di Bernardo, M.; Liu, Y.Y. Controlling complex networks with complex nodes. *Nat. Rev. Phys.* **2023**, *5*, 250–262. [[CrossRef](#)]
14. Shvydun, S. Models of similarity in complex networks. *PeerJ Comput. Sci.* **2023**, *9*, e1371. [[CrossRef](#)] [[PubMed](#)]
15. Huang, H.; Ren, J.; Alhudhaif, A.; Alenezi, F.; Xie, L.; Li, J. An efficient complex network embedding model for hierarchical networks. *Inf. Sci.* **2023**, *643*, 119226. [[CrossRef](#)]
16. Jiang, S.; Zhou, J.; Small, M.; Lu, J.a.; Zhang, Y. Searching for Key Cycles in a Complex Network. *Phys. Rev. Lett.* **2023**, *130*, 187402. [[CrossRef](#)] [[PubMed](#)]
17. Brown, G.G.; Cox, L.A., Jr. How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Anal.* **2011**, *31*, 196–204. [[CrossRef](#)]
18. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending Critical Infrastructure. *Interfaces* **2006**, *36*, 530–544. [[CrossRef](#)]
19. Li, Y.P.; Tan, S.Y.; Deng, Y.; Wu, J. Attacker-defender game from a network science perspective. *Chaos Interdiscip. J. Nonlinear Sci.* **2018**, *28*, 051102. [[CrossRef](#)]
20. Li, Y.P.; Deng, Y.; Xiao, Y.; Wu, J. Attack and Defense Strategies in Complex Networks Based on Game Theory. *J. Syst. Sci. Complex.* **2019**, *32*, 1630–1640. [[CrossRef](#)]
21. Li, Y.P.; Xiao, Y.; Li, Y.; Wu, J. Which Targets to Protect in Critical Infrastructures—A Game-Theoretic Solution from a Network Science Perspective. *IEEE Access* **2018**, *6*, 56214–56221. [[CrossRef](#)]
22. Chaoqi, F.; Pengtao, Z.; Lin, Z.; Yangjun, G.; Na, D. Camouflage strategy of a Stackelberg game based on evolution rules. *Chaos Solitons Fractals* **2021**, *153*, 111603. [[CrossRef](#)]
23. Gu, X.; Zeng, C.; Xiang, F. Applying a Bayesian Stackelberg game to secure infrastructure system: From a complex network perspective. In Proceedings of the 2019 4th International Conference on Automation, Control and Robotics Engineering, Shenzhen, China, 19–21 July 2019.
24. Jiang, J.; Liu, X. Bayesian Stackelberg game model for water supply networks against interdictions with mixed strategies. *Int. J. Prod. Res.* **2021**, *59*, 2537–2557. [[CrossRef](#)]
25. Zeng, C.; Ren, B.; Li, M.; Liu, H.; Chen, J. Stackelberg game under asymmetric information in critical infrastructure system: From a complex network perspective. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 083129. [[CrossRef](#)] [[PubMed](#)]
26. Zeng, C.; Ren, B.; Liu, H.; Chen, J. Applying the Bayesian Stackelberg Active Deception Game for Securing Infrastructure Networks. *Entropy* **2019**, *21*, 909. [[CrossRef](#)]
27. Thompson, K.H.; Tran, H.T. Application of a Defender-Attacker-Defender Model to the U.S. Air Transportation Network. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018; pp. 1–5. [[CrossRef](#)]
28. Thompson, K.H.; Tran, H.T. Operational Perspectives into the Resilience of the U.S. Air Transportation Network against Intelligent Attacks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 1503–1513. [[CrossRef](#)]
29. Yuan, W.; Zeng, B. Cost-effective power grid protection through defender–attacker–defender model with corrective network topology control. *Energy Syst.* **2020**, *11*, 811–837. [[CrossRef](#)]
30. Abidi, M.H.; Alkhalefah, H.; Moiduddin, K.; Al-Ahmari, A. Novel improved chaotic elephant herding optimization algorithm-based optimal defense resource allocation in cyber-physical systems. *Soft Comput.-Fusion Found. Methodol. Appl.* **2023**, *27*, 2965–2980. [[CrossRef](#)]
31. Benisha, R.B.; Ratna, S.R. A two-step trace model for the detection of UVI attacks against power grids in the wireless network. *Soft Comput.-Fusion Found. Methodol. Appl.* **2021**, *25*, 5199–5207. [[CrossRef](#)]
32. Li, Y.L.; Su, H.; Zhang, C.; Li, H.J.; Lin, J.; Li, G.J. Research on network protection strategy of associated infrastructure based on incomplete information game. *Syst. Eng.-Theory Pract.* **2022**, *42*, 1026–1042.
33. Wang, Z.G.; Lu, Y.; Li, X. Active defense strategy selection of military information network based on incomplete information game. *Acta Armamentarii* **2020**, *41*, 608–617.
34. Jiang, M.T. Research on Network Defense Resource Scheduling Strategy of Critical Infrastructure Systems Based on Game Theory. Master’s Thesis, Hangzhou Dianzi University, Hangzhou, China, 2022.
35. Cauteruccio, F.; Terracina, G.; Ursino, D. Generalizing identity-based string comparison metrics: Framework and techniques. *Knowl.-Based Syst.* **2020**, *187*, 104820. [[CrossRef](#)]
36. Atanassov, K.T. Intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1986**, *20*, 87–96. [[CrossRef](#)]
37. Delgado, M.; Vila, M.A.; Voxman, W. On a canonical representation of fuzzy numbers. *Fuzzy Sets Syst.* **1998**, *93*, 125–135. [[CrossRef](#)]
38. Angelov, P.P. Optimization in an intuitionistic fuzzy environment. *Fuzzy Sets Syst.* **1997**, *86*, 299–306. [[CrossRef](#)]
39. Aggarwal, A.; Mehra, A.; Chandra, S. Application of linear programming with I-fuzzy sets to matrix games with I-fuzzy goals. *Fuzzy Optim. Decis. Mak.* **2012**, *11*, 465–480. [[CrossRef](#)]

40. Nan, J.X.; Li, D.F. Linear programming approach to matrix games with intuitionistic fuzzy goals. *Int. J. Comput. Intell. Syst.* **2013**, *6*, 186–197. [[CrossRef](#)]
41. Li, D.F.; Nan, J.X. A nonlinear programming approach to matrix games with payoffs of atanassov's intuitionistic fuzzy sets. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **2009**, *17*, 585–607. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.