TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 27/31 pp384–401
DOI: 10.26599/TST.2024.9010063
Volume 30, Number 1, February 2025

Attack and Defense Game with Intuitionistic Fuzzy Payoffs in Infrastructure Networks

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

Abstract: Due to our increasing dependence on infrastructure networks, the attack and defense game in these networks has draw great concerns from security agencies. Moreover, when it comes to evaluating the payoffs in practical attack and defense games in infrastructure networks, the lack of consideration for the fuzziness and uncertainty of subjective human judgment brings forth significant challenges to the analysis of strategic interactions among decision makers. This paper employs intuitionistic fuzzy sets (IFSs) to depict such uncertain payoffs, and introduce a theoretical framework for analyzing the attack and defense game in infrastructure networks based on intuitionistic fuzzy theory. We take the changes in three complex network metrics as the universe of discourse, and intuitionistic fuzzy sets are employed based on this universe of discourse to reflect the satisfaction of decision makers. We employ an algorithm based on intuitionistic fuzzy theory to find the Nash equilibrium, and conduct experiments on both local and global networks. Results show that: (1) the utilization of intuitionistic fuzzy sets to depict the payoffs of attack and defense games in infrastructure networks can reflect the unique characteristics of decision makers' subjective preferences. (2) the use of differently weighted proportions of the three complex network metrics has little impact on decision makers' choices of different strategies.

Key words: infrastructure networks; attack and defense game; intuitionistic fuzzy set; Nash equilibrium

1 Introduction

Infrastructure networks such as power grids, transportation systems, communication networks, and water supply networks play a vital role in modern society. These networks consist of interconnected and interdependent nodes, ranging in number from a few dozen to several thousand. With the rapid trend towards the networking of human society, the dysfunction of critical infrastructure networks could have a significant negative impact on people's lives and property[1]. Traditional complex network theory can help in employing attack and defense strategies from the perspective of network topology, such as network disintegration[2–5] and protection[6–8]; however, it is difficult to use these conventional methods when dealing with deliberate opponents.

Game theory offers an effective framework for studying the optimal strategies for the players in these interactions, in which conflicts are represented with mathematical methods[9–11]. Brown et al.[12, 13] utilized game theory to analyze military strikes and homeland defense. Notably, they investigated dynamic game models through bi-level and tri-level planning models, and examined optimal attack strategies under three different defense scenarios: No defense, key node protection, and three-quarters node protection[14]. Li et al.[15–17] applied the attack and defense game model to complex networks, studying the correlations

• Yibo Dong, Jin Liu, Jiaqi Ren, Zhe Li, and Weili Li are with Science and Technology on Information Systems Engineering Laboratory, National University of Defense Technology, Changsha 410073, China. E-mail: dongyibo@nudt.edu.cn; liujin229234@nudt.edu.cn; jiaqiren@nudt.edu.cn; lizhe@nudt.edu.cn; weiwei6563@nudt.edu.cn.

* To whom correspondence should be addressed.

Manuscript received: 2023-10-11; revised: 2024-02-28; accepted: 2024-03-25

between equilibrium strategies and cost sensitivity in a scale-free network and evaluating the effects of cost constraints and sensitivity on the equilibrium results. Fu et al.[18] developed a static network attack and defense game model to examine the impact of cascading failures, and established a dynamic game model based on camouflage strategies. In addition, they proposed an evolutionary rule to optimize camouflage strategies and achieve optimal resource allocation[19]. Gu et al.[20] analyzed the significance of the Bayesian Stackelberg game model from the perspective of network science. Zeng et al.[21, 22] also applied the Bayesian Stackelberg game model, and proposed a false network construction method. In their study, they focused on the allocation of resources for defending critical infrastructure networks under conditions of asymmetric information. Thompson and Tran[23, 24] analyzed the potential impacts of intelligent attacks and worst-case interruptions to the US air transportation network; they then established a defender-attacker-defender optimization model with three levels, and proceeded to solve it. Qi et al.[25, 26] proposed a link-hiding rule and analyzed its impact in terms of optimization within the context of dynamic attack and defense games played out on complex networks. Huang et al.[27] used sequential game theory to model the attack and defense games on complex networks, and proposed a strategy optimization method. Tan et al.[28] innovate a moving target defense decision method based on evolutionary game and Wright-Fisher process from the perspective of bounded rationality of both attack-defense. Zhang et al.[29] introduced a novel real-time defense decision method based on differential game theory for complex networks, demonstrating improved defense performance and practicality compared to existing approaches; they then proposed a globally optimal defense decision method aligned with the overall network defense objective by combining differential game theory with complex network characteristics[30].

However, there are two main challenges on the research studies described above. Firstly, there are several qualitative, uncertain, and imprecise factors in attack and defense games, such as the decision makers' preferences and willingness, which can significantly affect their behavior and satisfaction. Hence, when considering the practical attack and defense games in infrastructure networks, a more appropriate definition for the payoff would be "satisfaction with the achievement of the goal". An appropriate method is required to construct the payoff matrices by adopting this definition and to obtain the Nash equilibrium. Secondly, a single reference metric has been used to evaluate network performance, as the majority of current studies on attack and defense games in infrastructure networks have employed only one metric as a reference for calculating payoffs. In most instances, the size of the largest connected component is selected. However, this method can only reflect certain aspects of the characteristics of the network, and does not encompass the multifaceted considerations of decision makers in terms of network performance. Consequently, it becomes challenging to reflect the comprehensive network performance when creating payoff matrices.

To address the first of limitations, we define the payoffs based on the satisfaction with the achievement of the goal in an attack and defense game. In regard to the fuzziness and uncertainty of human judgment, it is often impossible in practice to model these using probability theory. Fortunately, the fuzzy set theory was proposed by Zadeh[31] in 1965 provides a useful tool for handling such problems. The notion of fuzzy sets was further extended to intuitionistic fuzzy sets (IFS) by Atanassov[32, 33]. The application of the intuitionistic fuzzy theory is highly extensive[34–36], and the major advantage of IFSs over fuzzy sets is that an IFS separates the degree of acceptance from the degree of non-acceptance of a decision. Due to this advantage, IFS theory can describe the preference and willingness of decision makers in an attack and defense game more comprehensively[37, 38]. In addition, when varying types of decision makers are involved, a perspective known as an optimistic and pessimistic approach is possible, where some flexibility is allowed through the use of elastic boundaries[39–43].

To deal with the second limitation, we consider three network performance evaluation metrics: The size of the largest connected component[44], the network efficiency[45], and the clustering coefficient[46]. These metrics are used to measure the network connectivity, the efficiency of information transmission, and the tightness of the node connections, respectively. We use appropriate membership/non-membership functions (MFs/NFs) to calculate initial IFS payoff matrices based on these three distinct metrics, separately. The final IFS payoff matrix is then obtained by aggregating these initial IFS payoff matrices with different weight distributions. In this way, the structural features and functional effects of the networks can be described more comprehensively in terms of payoffs.

In this paper, we propose a model for an attack and defense game with intuitionistic fuzzy payoffs in infrastructure networks. Our model employs appropriate MFs/NFs to facilitate the decision-making process, and enables decision makers to consider multiple metrics for a comprehensive evaluation. In addition, a method of constructing payoff matrices and obtaining the Nash equilibrium is presented. In our experiments, we explore two scenarios involving local and global networks. The results obtained for both scenarios indicate that these complex network metrics have distinct effects, which may influence the Nash equilibrium. Moreover, it is shown that IFS theory can be effectively integrated with attack and defense games in infrastructure networks to reflect the decision makers' subjective preferences.

The rest of the article is organized as follows. In Section 2, some definition and preliminaries related to IFS theory are reviewed. Section 3 explains the cost model, strategies, objective payoffs, and the conversion of intuitive fuzzy preferences. The solution method for the game is introduced in Section 4. Section 5 presents some experimental equilibrium results for local and global networks. Finally, our conclusions are summarized in Section 6.

2 Preliminary

Some basic concepts relating to IFSs, MFs/NFs, and the optimistic/pessimistic approach are introduced in this section.

2.1 Intuitionistic fuzzy sets

An IFS A in a universe of discourse U is a set of ordered triplets[32]: $(x,\mu_A(x),\nu_A(x))|x\in U$, where $\mu_A(x):U\to[0,1]$ (MF) and $\nu_A(x):U\to[0,1]$ (NF) are functions such that $\forall x\in U$, $0\leqslant\mu_A(x)+\nu_A(x)\leqslant 1$. It can be observed that the membership function (MF) demonstrates the relationship between membership (μ_A) and the variation of x, while the non-membership function (NF) illustrates the relationship between non-membership (ν_A) and the variation of x. The expression $(1-\mu_A(x)-\nu_A(x))$ represents the degree of hesitation of $x\in U$.

2.2 Hyperbolic membership and non-membership functions

The shape of the hyperbolic MF has a concave segment in one part, and is convex for the remainder. Marginal rate or marginal effect refer to the change in one variable resulting from a unit change in another variable, and they often represent the slope or gradient of the relationship between two variables at a specific point. When decision makers are worse off with respect to a goal, they tend to have a higher marginal rate of satisfaction with respect to that goal, and the convex shape captures this behavior in regard to the MF. On the other hand, when decision makers are better off with respect to a goal, they tend to have a smaller marginal rate of satisfaction, and this behavior is modeled using the concave portion of the membership function. While the dissatisfaction of decision makers, represented by NF, is conversely expressed. The hyperbolic MFs/NFs are given by Refs. [47, 48] as Eqs. (1) and (2), where $\alpha^{\text{acc}}=\dfrac{6}{m_H^{\text{acc}}-n_H^{\text{acc}}}$; m_H^{acc} indicates maximum acceptable level; n_H^{acc} indicates the minimum acceptable level; $\alpha^{\text{rej}}=\dfrac{6}{m_H^{\text{rej}}-n_H^{\text{rej}}}$; m_H^{rej} indicates the maximum rejectable level; and n_H^{rej} indicates the minimum rejectable level.

$$\mu_H(x)=\begin{cases}0, & \text{if } x<n_H^{\text{acc}};\\ \dfrac{1}{2}\tanh\left(\alpha^{\text{acc}}\left(x-\dfrac{m_H^{\text{acc}}+n_H^{\text{acc}}}{2}\right)\right)+\dfrac{1}{2}, & \text{if } n_H^{\text{acc}}\leqslant x\leqslant m_H^{\text{acc}};\\ 1, & \text{if } x>m_H^{\text{acc}}\end{cases}\tag{1}$$

$$\nu_H(x)=\begin{cases}1, & \text{if } x<n_H^{\text{rej}};\\ \dfrac{1}{2}\tanh\left(\alpha^{\text{rej}}\left(\dfrac{m_H^{\text{rej}}+n_H^{\text{rej}}}{2}-x\right)\right)+\dfrac{1}{2}, & \text{if } n_H^{\text{rej}}\leqslant x\leqslant m_H^{\text{rej}};\\ 0, & \text{if } x>m_H^{\text{rej}}\end{cases}\tag{2}$$

2.3 Exponential membership and non-membership functions

An exponential MF represents the situation when decision makers are worse off with respect to an objective and opts for a higher marginal rate of satisfaction. When choosing an exponential MF, a decision maker can also choose to reduce duality gaps by selecting appropriate shape parameters for the construction of the MF. While the dissatisfaction of decision makers, represented by NF, is conversely expressed. The exponential MFs/NFs can be defined as Eqs. (3) and (4), where t is a parameter set by the decision maker. When $t>0$, $\mu_E(x)$ is a convex function that exhibits a monotonic increasing marginal effect. Conversely, when $t<0$, the marginal effect monotonically decreases. m_E^{acc} indicates the highest acceptable level; n_E^{acc} indicates the lowest acceptable level; m_E^{rej} indicates the highest rejectable level; and n_E^{rej} indicates the lowest rejectable level.

$$\mu_E(x)=\begin{cases}0, & \text{if } x<n_E^{\mathrm{acc}};\\ \dfrac{\mathrm{e}^{\frac{-t(m_E^{\mathrm{acc}}-x)}{m_E^{\mathrm{acc}}-n_E^{\mathrm{acc}}}}-\mathrm{e}^{-t}}{1-\mathrm{e}^{-t}}, & \text{if } n_E^{\mathrm{acc}}\leqslant x\leqslant m_E^{\mathrm{acc}};\\ 1, & \text{if } x>m_E^{\mathrm{acc}}\end{cases}\tag{3}$$

$$\nu_E(x)=\begin{cases}1, & \text{if } x<n_E^{\mathrm{rej}};\\ 1-\dfrac{\mathrm{e}^{\frac{-t(m_E^{\mathrm{rej}}-x)}{m_E^{\mathrm{rej}}-n_E^{\mathrm{rej}}}}-\mathrm{e}^{-t}}{1-\mathrm{e}^{-t}}, & \text{if } n_E^{\mathrm{rej}}\leqslant x\leqslant m_E^{\mathrm{rej}};\\ 0, & \text{if } x>m_E^{\mathrm{rej}}\end{cases}\tag{4}$$

2.4 Optimistic approach

In an optimistic approach, the combination of MFs/NFs is perturbed to accommodate more or reject less than the normal approach. This can be done by reducing the complete rejection range (i.e., $\nu(x)=1$) and hence displaying an optimistic trend. Here, an interval beyond $[n_H^{\mathrm{rej}},m_H^{\mathrm{rej}}]$ is obtained in which the acceptance is low but complete rejection is avoided. For example, a combination with a tolerance of $\varepsilon>0$ under conditions of hyperbolic MFs/NFs[41, 42] is given in Eqs. (5) and (6), where $\alpha^{\mathrm{acc}}=\dfrac{6}{m_H^{\mathrm{acc}}-m_H^{\mathrm{acc}}}$; $\alpha^{\mathrm{rej}}=\dfrac{6}{m_H^{\mathrm{rej}}+\varepsilon-n_H^{\mathrm{rej}}}$. We illustrate them in Fig. 1.

$$\mu^{\mathrm{opt}}(x)=\begin{cases}0, & \text{if } x<n_H^{\mathrm{acc}};\\ \dfrac{1}{2}\tanh\left(\alpha^{\mathrm{acc}}\left(x-\dfrac{m_H^{\mathrm{acc}}+n_H^{\mathrm{acc}}}{2}\right)\right)+\dfrac{1}{2}, & \text{if } n_H^{\mathrm{acc}}\leqslant x\leqslant m_H^{\mathrm{acc}};\\ 1, & \text{if } x>m_H^{\mathrm{acc}}\end{cases}\tag{5}$$

$$\nu^{\mathrm{opt}}(x)=\begin{cases}1, & \text{if } x<n_H^{\mathrm{rej}}-\varepsilon;\\ \dfrac{1}{2}\tanh\left(\alpha^{\mathrm{rej}}\left(\dfrac{m_H^{\mathrm{rej}}+n_H^{\mathrm{rej}}-\varepsilon}{2}-x\right)\right)+\dfrac{1}{2}, & \text{if } n_H^{\mathrm{rej}}-\varepsilon\leqslant x\leqslant m_H^{\mathrm{rej}};\\ 0, & \text{if } x>m_H^{\mathrm{rej}}\end{cases}\tag{6}$$

$$\mu^{\mathrm{pes}}(x)=\begin{cases}0, & \text{if } x\leqslant n_H^{\mathrm{acc}}+\varepsilon';\\ \dfrac{1}{2}\tanh\left(\alpha^{\mathrm{acc}}\left(x-\dfrac{m_H^{\mathrm{acc}}+n_H^{\mathrm{acc}}+\varepsilon'}{2}\right)\right)+\dfrac{1}{2}, & \text{if } n_H^{\mathrm{acc}}+\varepsilon'<x\leqslant m_H^{\mathrm{acc}};\\ 1, & \text{if x > }\mathrm{m}_H^{\mathrm{acc}}\end{cases}\tag{7}$$

$$\nu^{\mathrm{pes}}(x)=\begin{cases}1, & \text{if } x\leqslant n_H^{\mathrm{rej}};\\ \dfrac{1}{2}\tanh\left(\alpha^{\mathrm{rej}}\left(\dfrac{m_H^{\mathrm{rej}}+n_H^{\mathrm{rej}}}{2}-x\right)\right)+\dfrac{1}{2}, & \text{if } n_H^{\mathrm{rej}}<x\leqslant m_H^{\mathrm{rej}};\\ 0, & \text{if } x>\mathrm{m}_H^{\mathrm{rej}}\end{cases}\tag{8}$$

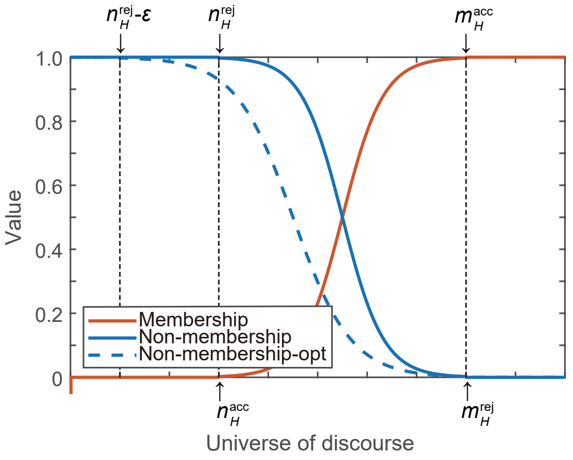


Fig. 1 Hyperbolic MF/NF in optimistic sense.

2.5 Pessimistic approach

In a pessimistic approach, the combination of MFs/NFs is modified in order to accept less or reject more than the normal approach. This can be done by reducing the range of acceptance (i.e., $\mu(x)\neq 0$). Hence, a proposed possible combination with a tolerance of ε', where $0<\varepsilon'<(m_H^{\mathrm{acc}}-n_H^{\mathrm{acc}})$, for hyperbolic MFs/NFs[49] can be expressed as Eqs. (7) and (8), where $\alpha^{\mathrm{acc}}=\dfrac{6}{m_H^{\mathrm{acc}}-n_H^{\mathrm{acc}}-\varepsilon'}$; $\alpha^{\mathrm{rej}}=\dfrac{6}{m_H^{\mathrm{rej}}-n_H^{\mathrm{rej}}}$. We illustrate them in Fig. 2.

2.6 Intuitionistic fuzzy weighted arithmetic average operator

Let $A_1,A_2,\ldots,A_n$ represent n IFSs, where $A_j=\{\langle x,\mu_{A_j}(x),\nu_{A_j}(x)\rangle \mid x\in U\}\,(j=1,2,\ldots,n).\omega=(\omega_1,\omega_2,\ldots,\omega_n)^{\mathrm{T}}$ is the weight vector of $A_j(j=1,2,\ldots,n)$, where $\omega_j\geqslant 0$, $\sum\limits_{j=1}^{n}\omega_j=1$. The intuitionistic fuzzy weighted

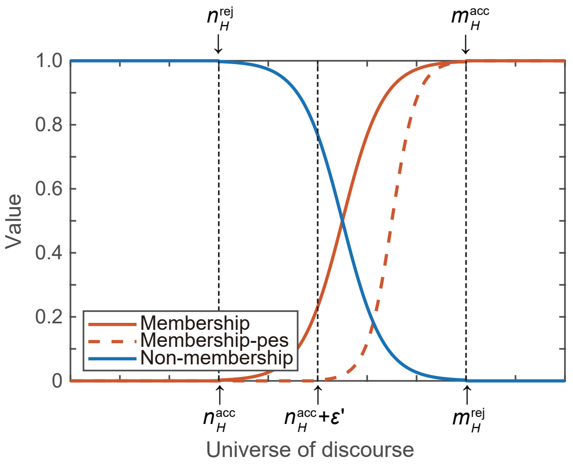


Fig. 2 Hyperbolic MF/NF in pessimistic sense.

average aggregation (IFWAA) operator is then defined as follows[50, 51]:

$$\begin{aligned}&\mathrm{IFWAA}_{\omega}(A_1,A_2,\ldots,A_n)=\\&\omega_1A_1\oplus\omega_2A_2\oplus\ldots\oplus\omega_nA_n=\\&\sum_{j=1}^{n}\omega_jA_j\end{aligned}\tag{9}$$

$$\begin{aligned}&\mathrm{IFWAA}_{\omega}(A_1,A_2,\ldots,A_n)=\\&\left\{\langle x,1-\prod_{j=1}^{n}\left(1-\mu_{A_j}(x)\right)^{\omega_j},\right.\\&\left.\prod_{j=1}^{n}\left(\nu_{A_j}(x)\right)^{\omega_j}\rangle\mid x\in U\right\}\end{aligned}\tag{10}$$

We can rewrite Eq. (9) as Eq. (10).

3 Attack and Defense Game Model Based on Intuitionistic Fuzzy Theory

Based on intuitionistic fuzzy theory, we construct an attack and defense game model for infrastructure networks. Before constructing this models, the corresponding notations are illustrated as Table 1.

3.1 Basic assumptions

The following assumptions are made in this model:

(1) There is only one attacker, who aims to attack some nodes in the target network to degrade the performance of the system, and one defender, who aims to maintain the functionality of the network by protecting a subset of nodes. The attached edges will be removed if one node fails.

(2) Both players can obtain complete information about the target network and have full knowledge of the opponent, meaning that they are perfectly informed of all the possible strategies that the opponent may adopt and the payoffs to each player for each strategy profile.

(3) As the game is a simultaneous one, both the attacker and the defender move without knowing exactly which strategy the opponent will choose.

(4) The game is played in a single round and is not repeated over multiple rounds.

Table 1 Main notations used in this model.

Notation	Description
V	Set of nodes
E	Set of edges
c_i^A, c_i^D	Attack and defense cost
r_i	Referential property of node v_i, such as node degree
q_A, q_D	Attack and defense cost sensitivity parameters
θ_A, θ_D	Attack and defense cost constraint paremeters
C^A, C^D	Available resources of the attacker and defender
x_i, y_i	Parameters that determine the state of node v_i being attacked or defended
$C_{S_{A\tilde{i}}}, C_{S_{D\tilde{j}}}$	Total cost of attack strategy $S_{A\tilde{i}}$ and defense strategy $S_{D\tilde{j}}$
ω_A, ω_D	Minimum utilization rates of the available cost resources for the attacker and defender
U_k^A, U_k^D	Objective payoff matrices of the attacker and defender under the metric k
$U_k^{\mathrm{IA}}, U_k^{\mathrm{ID}}$	IFS payoff matrices of the attacker and defender

3.2 Strategies

Consider a target network, such as a railway network, that is formalized in terms of a simple undirected graph $G(V,E)$, where $V=\{v_1,v_2,...,v_N\}$ is the set of nodes and $E\subseteq V\times V$ is the set of edges (i.e., the railway stations and the railway lines in the railway network, respectively). Let $N=|V|$ be the number of nodes in the network. We define $A(G)=(a_{ij})_{N\times N}$ as the adjacency matrix of G, where $a_{ij}=a_{ji}=1$ if nodes v_i and v_j are adjacent, and $a_{ij}=a_{ji}=0$ otherwise.

For node v_i, let c_i^A and c_i^D be the attack cost and defense cost, respectively. The cost c_i^A or c_i^D is a function of a certain referential property $r_i\geqslant 0$ of node v_i, which can be expressed as

$$c_i^A=r_i^{q_A}\tag{11}$$

$$c_i^D=r_i^{q_D}\tag{12}$$

where $q_A\geqslant 0$ is the attack cost sensitivity parameter, and $q_D\geqslant 0$ is the defense cost sensitivity parameter. The parameters q_A and q_D can be obtained based on expert experience and historical information. In this paper, the referential property r_i is set as the degree of the nodes. In particular, when $q_A=q_D=0$, the resource consumption for the attack or defense of different nodes is the same.

The available resources of both the attacker and the defender are defined as

$$C^A=\theta_A\sum_{i=1}^{N}c_i^A=\theta_A\sum_{i=1}^{N}r_i^{q_A}\tag{13}$$

$$C^D=\theta_D\sum_{i=1}^{N}c_i^D=\theta_D\sum_{i=1}^{N}r_i^{q_D}\tag{14}$$

The attack and defense cost constraint parameters are denoted by $\theta_A\in[0,1]$ and $\theta_D\in[0,1]$, respectively. The values of θ_A and θ_D represent the attacker's and defender's respective cost budgets for attacking or defending.

Based on the cost model presented above and existing studies[21, 25, 51] of the definitions of feasible strategies under non-uniform cost constraints, it is apparent that existing definitions of feasible strategies can only be applied to some typical strategies, rather than to all feasible strategies. Taking the attacker as an example, the feasible strategies in former studies are defined as follows.

Suppose $S_{A\tilde{i}} = [x_1, x_2, ..., x_N] \in S_A$ is an attack strategy vector, where S_A represents the strategy set of the attacker. We define $V_A \subseteq V$ as the set of attacked nodes, and let $x_i = 1$ if node v_i is attacked ($v_i \in V^A$); otherwise, $x_i = 0$. The total cost of an attack strategy $S_{A\tilde{i}}$ is denoted by

$$C_{S_{A\tilde{i}}} = \sum_{v_i \in V^A} c_i^A = \sum_{i=1}^{N} x_i c_i^A = \sum_{i=1}^{N} x_i r_i^{qA} \tag{15}$$

The cost constraint on the attacker is

$$C_{S_{A\tilde{i}}} = \sum_{i=1}^{N} x_i r_i^{qA} \leqslant C^A = \theta_A \sum_{i=1}^{N} r_i^{qA} \tag{16}$$

To obtain feasible strategies based on the constraint described above, we could select the fewest possible attack nodes to satisfy the constraint. However, in practical situations, there will be a lower bound on the attacker's resources for attacking nodes. This lower bound is essential to enable the attacker to achieve the goal. To address this conflict, we propose the concept of a minimum resource utilization rate. ω_A and ω_D represent the minimum utilization rates of the available cost resources for the attacker and defender, respectively. For the attacker, the overall constraint can be expressed as follows:

$$\omega_A \theta_A \sum_{i=1}^{N} r_i^{qA} \leqslant C_{S_{A\tilde{i}}} = \sum_{i=1}^{N} x_i r_i^{qA} \leqslant C^A = \theta_A \sum_{i=1}^{N} r_i^{qA} \tag{17}$$

Similarly, the defense strategy vector is expressed by $S_{D\tilde{j}} = [y_1, y_2, ..., y_N] \in S_D$, and the constraint on the defender is

$$\omega_D \theta_D \sum_{i=1}^{N} r_i^{qD} \leqslant C_{S_{D\tilde{j}}} = \sum_{i=1}^{N} y_i r_i^{qD} \leqslant C^D = \theta_D \sum_{i=1}^{N} r_i^{qD} \tag{18}$$

We assume that node v_i is removed only if it is attacked without being protected, i.e., $x_i = 1$ and $y_i = 0$. Conversely, the node will not be removed if it is defended ($y_i = 1$).

The attack and defense strategies defined in Formulas (17) and (18) refer to a vast strategy space, particularly for a large network size N. In real-world scenarios, it can be intuitively seen that the attacker and defender generally consider three types of strategy[2]:

(1) High degree strategy (HS). In this case, the attacker and defender allocate all their resources to the nodes with the highest degree. Although the number of nodes selected is small, they have a relatively high importance.

(2) Random strategy (RS). In this case, the attacker and defender allocate all their resources to nodes in a random manner.

(3) Low degree strategy (LS). In this scenario, the attacker and defender allocate all their resources to nodes with the lowest degree. Although the selected nodes may have a lower importance, their quantity is greater.

3.3 Payoffs

In this paper, we consider three metrics, the size of the largest connected component, the network efficiency, and the clustering coefficient, to evaluate the performance of complex networks.

(1) The size of the largest connected component is used to measure the connectivity of the network, and can be expressed as

$$\Gamma = \max(|C_1|, |C_2|, ..., |C_t|) \tag{19}$$

where $C_i\ (i = 1, 2, \ldots, t)$ represents the connected subgraphs.

(2) The network efficiency measures the speed of transmission of network information, and can be calculated as follows:

$$E = \frac{2}{N(N-1)} \sum_{1 \leqslant i \leqslant j \leqslant N} \frac{1}{D_{ij}} \tag{20}$$

where D_{ij} represents the shortest path between a pair of nodes v_i and v_j.

(3) The clustering coefficient is adopted to measure the degree of node clustering in the network, and can be expressed as Ref. [52],

$$H = \frac{1}{N} \sum_{i=1}^{N} \frac{K}{\frac{|N_i| \times (|N_i| - 1)}{2}} \tag{21}$$

where N_i is the set of nodes adjacent to v_i, and K is the actual number of edges formed by the set N_i in the network.

Let $\hat{V} \subseteq V$ be the set of failing nodes, and $\hat{E}$ be the corresponding set of removed edges. After a round of the game, the network can be denoted by $\hat{G} = (V, E - \hat{E})$. We define $U_k^A : |S_A| \times |S_D|$ as the objective payoff matrix of the attacker when the attacker adopts strategy S_A and the defender adopts strategy S_D under the metric k. Similarly, the objective payoff matrix of the defender is defined as $U_k^D(S_A, S_D)$. We then have

$$U_k^A(S_A, S_D) = \frac{M_k(G) - M_k(\hat{G})}{M_k(G)} \in [0,1] \tag{22}$$

$$U_k^D(S_A, S_D) = \frac{M_k(\hat{G}) - M_k(G)}{M_k(G)} \in [-1,0] \tag{23}$$

where M_1, M_2, and M_3 denote the size of the largest connected component, the network efficiency, and the clustering coefficient for the network, respectively.

Let $u_{\tilde{i}\tilde{j}}^k = U_k^A\left(S_{A\tilde{i}}, S_{D\tilde{j}}\right)$; $m = |S_A|$; $n = |S_D|$; $1 \leqslant \tilde{i} \leqslant m$; $1 \leqslant \tilde{j} \leqslant n$, where U_k^A is expressed as follows:

$$U_k^A = \begin{array}{c} \\ S_{A1} \\ S_{A2} \\ \vdots \\ S_{Am} \end{array} \begin{array}{c} \begin{array}{cccc} S_{D1} & S_{D2} & \cdots & S_{Dn} \end{array} \\ \begin{pmatrix} u_{11}^k & u_{12}^k & \cdots & u_{1n}^k \\ u_{21}^k & u_{22}^k & \cdots & u_{2n}^k \\ \vdots & \vdots & & \vdots \\ u_{m1}^k & u_{m2}^k & \cdots & u_{mn}^k \end{pmatrix} \end{array} \tag{24}$$

We note that $U_k^A(S_A, S_D) + U_k^D(S_A, S_D) = 0$, as the game is a two-player zero-sum game. Hence, U_k^D can be expressed as $-U_k^A$.

Due to the fuzziness and uncertainty arising from subjective factors and human judgments, it is more appropriate to define the payoff to a decision maker as "satisfaction with the achievement of the goal". In this paper, intuitionistic fuzzy theory is used to reflect the decision makers' preferences. We assume that the change in the complex network metrics ($u_{\tilde{i}\tilde{j}}^k$) represents the universe of discourse X, and "satisfaction with the achievement of the goal" is an IFS on X, denoted by $\langle \mu_{\tilde{i}\tilde{j}}^k, v_{\tilde{i}\tilde{j}}^k \rangle$. For the attacker, we transform the change in complex network metrics ($u_{\tilde{i}\tilde{j}}^k$) into an IFS $\langle \mu_{\tilde{i}\tilde{j}}^k, v_{\tilde{i}\tilde{j}}^k \rangle$ using an appropriate MF/NF, as described in Section 2. We then construct the initial IFS payoff matrices based on different metrics. As this is a zero-sum game, the defender's loss can be represented by the same IFS $\langle \mu_{\tilde{i}\tilde{j}}^k, v_{\tilde{i}\tilde{j}}^k \rangle$. The initial IFS payoff matrix for the attacker can then be represented as follows:

$$U_k^{\text{IA}} = \begin{array}{c} \\ S_{A1} \\ S_{A2} \\ \vdots \\ S_{Am} \end{array} \begin{array}{c} \begin{array}{cccc} S_{D1} & S_{D2} & \cdots & S_{Dn} \end{array} \\ \begin{pmatrix} <\mu_{11}^k, v_{11}^k> & <\mu_{12}^k, v_{12}^k> & \cdots & <\mu_{1n}^k, v_{1n}^k> \\ <\mu_{21}^k, v_{21}^k> & <\mu_{22}^k, v_{22}^k> & \cdots & <\mu_{2n}^k, v_{2n}^k> \\ \vdots & \vdots & & \vdots \\ <\mu_{m1}^k, v_{m1}^k> & <\mu_{m2}^k, v_{m2}^k> & \cdots & <\mu_{mn}^k, v_{mn}^k> \end{pmatrix} \end{array} \tag{25}$$

As decision makers of different types tend to show varying degrees of subjective preference, we consider both optimistic and pessimistic approaches in Section 2 to describe these subjective preferences for specific strategies and incorporate them into specific strategy profiles. For example, the attacker may have a preference for strategies that involve attacking node v_i. From the perspective of the game, this preference can be expressed as follows. The attacker believes that the payoff under the strategy profile $(S_{A\tilde{i}}, S_{D\tilde{j}})$ will not be too low, where $x_i = 1$ in $S_{A\tilde{i}}$ (node v_i is attacked) and $y_i = 1$ in $S_{D\tilde{j}}$ (node v_i is defended). Consequently, under the specific strategy profile $(S_{A\tilde{i}}, S_{D\tilde{j}})$, we have $U_k^A(S_{A\tilde{i}}, S_{D\tilde{j}}) \xrightarrow{\mu^{\text{opt}}, v^{\text{opt}}} U_k^{\text{IA}}(S_{A\tilde{i}}, S_{D\tilde{j}})$.

To comprehensively evaluate the changes in the overall performance of the target network after a round of the game, the initial IFS payoff matrices based on three metrics are aggregated using certain weight distributions through the IFWAA operator (Eq. (9)) to obtain the finial IFS payoff matrix as follows:

$$\begin{aligned} &U^{\text{IA}}(S_A, S_D) = \\ &\omega_1 U_1^{\text{IA}}(S_A, S_D) \oplus \omega_2 U_2^{\text{IA}}(S_A, S_D) \oplus \omega_3 U_3^{\text{IA}}(S_A, S_D) \end{aligned} \tag{26}$$

$$\begin{aligned} &U^{\text{ID}}(S_A, S_D) = \\ &\omega_1 U_1^{\text{ID}}(S_A, S_D) \oplus \omega_2 U_2^{\text{ID}}(S_A, S_D) \oplus \omega_3 U_3^{\text{ID}}(S_A, S_D) \end{aligned} \tag{27}$$

The process of generating the final IFS payoff matrix under this model is shown in Fig. 3, and a network with 10 nodes is shown as an example. In this figure, we only focus on one game result where the attacker and defender choose strategies involving red and blue nodes, respectively. An appropriate MF/NF is used to calculate the initial IFS payoff matrices based on three distinct single metrics, and the final IFS payoff matrix is then obtained by aggregating these initial IFS payoff matrices under different weight distributions.

4 Solution Method

In this section, we will derive the solution method for the model proposed in Section 3. To ensure a standardized and clear process for generating the IFS

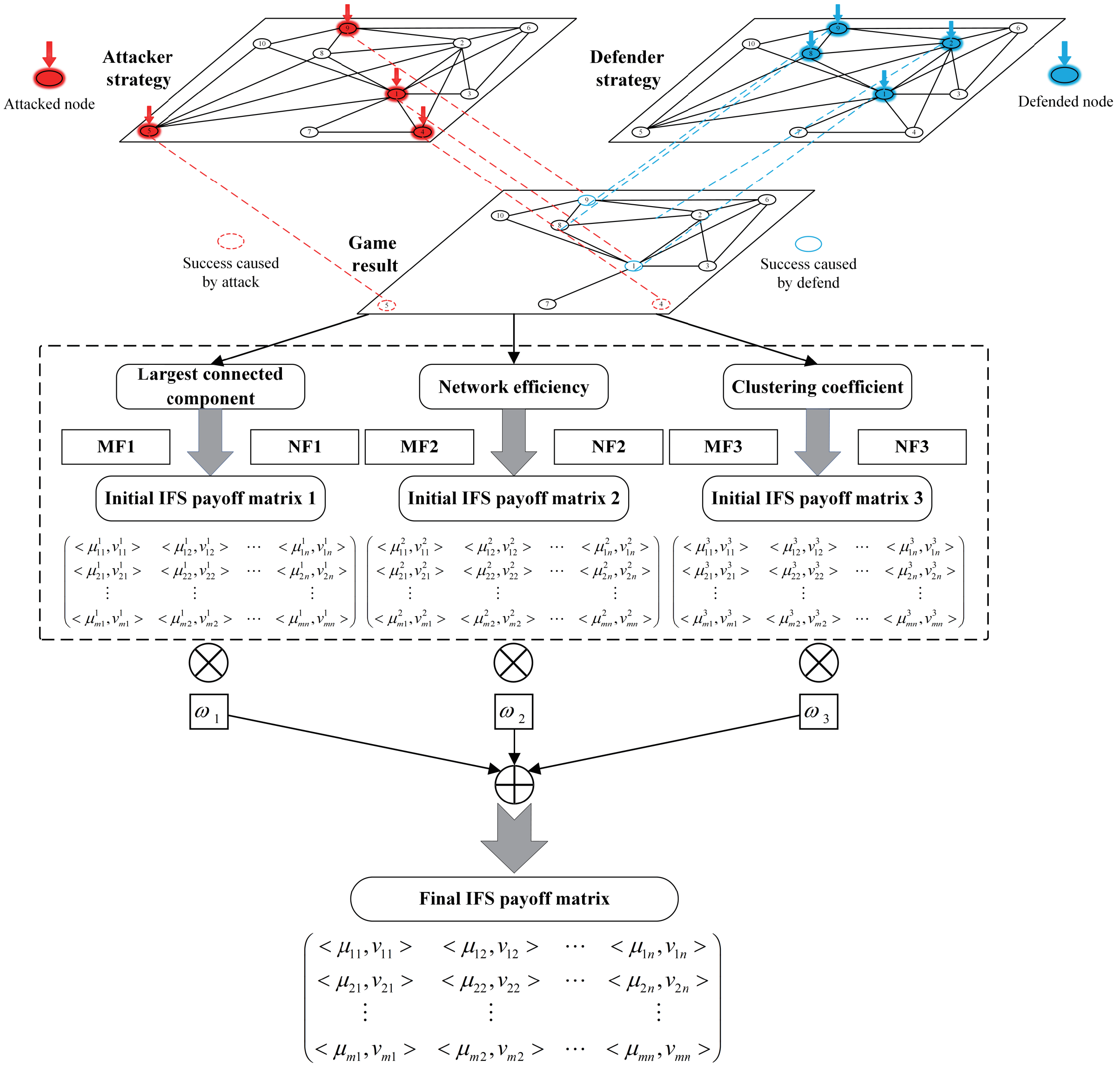


Fig. 3 Process used to generate the final IFS payoff matrix in the proposed game model.

payoff matrix, we first present an algorithm to obtain it. Subsequently, based on the IFS payoff matrices of both the attacker and defender, we introduce a methodology to determine the Nash equilibrium in this scenario. Furthermore, we also provide the method for calculating the equilibrium payoff value.

Pseudocode for obtaining the IFS payoff matrix of the attack and defense game in infrastructure networks is shown in Algorithm 1.

It should be noted that in Algorithm 1, when an RS is incorporated, it is imperative to use the average values for the payoffs, which means repeating Steps 6–7 many times to obtain the initial payoff matrices[15]. Nash equilibrium is a concept in game theory where each player in a strategic setting has chosen a strategy that no player can benefit by changing their strategy unilaterally, assuming that all other players' strategies remain constant. When the final IFS payoff matrix is obtained, a methodology is applied to obtain the Nash equilibrium of this zero-sum game based on a pair of nonlinear programming models[53], which are defined as Eqs. (28) and (29):

$$\min\{(1-\mu)^{\lambda}\nu^{1-\lambda}\};$$
$$\text{s.t.}\begin{cases}\prod_{i=1}^{|S_A|}[(1-\mu_{ij})^{\lambda}{\nu_{ij}}^{1-\lambda}]^{p_i}\leqslant(1-\mu)^{\lambda}\nu^{1-\lambda};\\ p_1+p_2+\cdots+p_{|S_A|}=1;\\ p_i\geqslant 0;\\ \mu\geqslant 0,\nu\geqslant 0;\\ 0\leqslant\mu+\nu\leqslant 1;\\ i=1,2,\ldots,|S_A|,j=1,2,\ldots,|S_D|\end{cases}\tag{28}$$

Algorithm 1 Pseudocode for obtaining the IFS payoff matrix

```
Input: A target network G(V, E) with $N = |V|$, $q_A, q_D, \theta_A, \theta_D, \omega_A, \omega_D$; $\mu_k(x)$, $\nu_k(x)$, $\mu_k^{\text{opt}}(x)$, $\nu_k^{\text{opt}}(x)$, $\mu_k^{\text{pes}}(x)$, $\nu_k^{\text{pes}}(x)$, specific strategy set $S_A^{\text{spe}}, S_D^{\text{spe}}$.
Output: The attacker's final IFS payoff matrix $U^{\text{IA}}$.
Calculate the degree $r_i$ for each node $v_i$ in the network $G(V,E)$;
Calculate the cost of each node in terms of attacking and defending: $c_i^A = r_i^{q_A}$, $c_i^D = r_i^{q_D}$;
Calculate the available resources for the attacker and defender: $C^A = \theta_A \sum_{i=1}^{N} c_i^A, C^D = \theta_D \sum_{i=1}^{N} c_i^D$;
Calculate the minimum resource utilization values for the attacker and the defender: $C_{\min}^A = \omega_A \theta_A \sum_{i=1}^{N} r_i^{q_A}, C_{\min}^D = \omega_D \theta_D \sum_{i=1}^{N} r_i^{q_D}$;
Enumerate all the attack strategies $S_{A\tilde{i}} \in S_A$ ($C_{\min}^A$ eqslant $C_{S_{A\tilde{i}}} \leqslant C^A$) and defense strategies $S_{D\tilde{j}} \in S_D$ ($C_{\min}^D \leqslant C_{S_{D\tilde{j}}} \leqslant C^D$); The strategies are determined by $\theta_A$, $\theta_D$, $\omega_A$, $\omega_D$ (for typical strategies HS, RS, LS, only $\theta_A$, $\theta_D$ are considered);
$U_k^A \leftarrow \text{zeros}(|S_A|, |S_D|)$;
Calculate the initial payoff matrices $U_k^A$ under each metric: $U_k^A(|S_A|, |S_D|) = \frac{M_k(G)-M_k(\hat{G})}{M_k(G)} \in [0,1] (k = 1,2,3)$;
$U_k^{IA} \xleftarrow{\mu_k(x), \nu_k(x)} U_k^A$;
for $i \leftarrow 1$ to $|S_A|$ do
    for $j \leftarrow 1$ to $|S_D|$ do
        if $S_{A\tilde{i}} \in S_A^{\text{spe}}$ and $S_{D\tilde{j}} \in S_D^{\text{spe}}$ then
            $U_k^{\text{IA}}(S_{A\tilde{i}}, S_{D\tilde{j}}) \xleftarrow{\mu_k^{\text{opt}}(x), \nu_k^{\text{opt}}(x)(\mu_k^{\text{pes}}(x), \nu_k^{\text{pes}}(x))} U_k^A(S_{A\tilde{i}}, S_{D\tilde{j}})$
        end
    end
end
Aggregate the initial IFS payoff matrices to obtain a final IFS payoff matrix $U^{\text{IA}}(S_A, S_D)$ using Eq. (26).
```

$$\max\{(1-\alpha)^{\lambda}\beta^{1-\lambda}\};$$
$$\text{s.t.}\begin{cases} \prod_{j=1}^{|S_D|} [(1-\mu_{ij})^{\lambda} {\nu_{ij}}^{1-\lambda}]^{q_i} \leqslant (1-\alpha)^{\lambda}\beta^{1-\lambda}; \\ q_1 + q_2 + \cdots + q_{|S_D|} = 1; \\ q_j \geqslant 0; \\ \alpha \geqslant 0, \beta \geqslant 0; \\ 0 \leqslant \alpha + \beta \leqslant 1; \\ i = 1, 2, \ldots, |S_A|, j = 1, 2, \ldots, |S_D| \end{cases} \tag{29}$$

where $\lambda \in [0,1]$ represents the relative weights of the constraints of the MF/NF. When λ has been determined, the Nash equilibrium $(\sigma_A, \sigma_D, \langle\mu,\nu\rangle, \langle\alpha,\beta\rangle)$ can be obtained. The probability vector for the attacker's mixed-strategy Nash equilibrium is denoted by $\sigma_A = \left(p_1, p_2, \ldots, p_{|S_A|}\right)^{\text{T}}$, while that of the defender is denoted by $\sigma_D = \left(q_1, q_2, \ldots, q_{|S_D|}\right)^{\text{T}}$. In addition, let $\langle\mu,\nu\rangle$ denote the equilibrium payoff value for the attacker in the game, while $\langle\alpha,\beta\rangle$ represents that of the defender. Both the equilibrium payoff values can be expressed as IFSs. The equilibrium payoff value for the attacker is defined as

$$E(\sigma_A, \sigma_D) = {\sigma_A}^{\text{T}} U^A \sigma_D =$$
$$\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_{|S_A|} \end{pmatrix}^{\text{T}} \begin{pmatrix} \langle\mu_{11},\nu_{11}\rangle & \langle\mu_{12},\nu_{12}\rangle & \cdots & \langle\mu_{1|S_D|},\nu_{1|S_D|}\rangle \\ \langle\mu_{21},\nu_{21}\rangle & \langle\mu_{22},\nu_{22}\rangle & \cdots & \langle\mu_{2|S_D|},\nu_{2|S_D|}\rangle \\ \vdots & \vdots & & \vdots \\ \langle\mu_{|S_A|1},\nu_{|S_A|1}\rangle & \langle\nu_{|S_A|2},\nu_{|S_A|2}\rangle & \cdots & \langle\nu_{|S_A||S_D|},\nu_{|S_A||S_D|}\rangle \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_{|S_D|} \end{pmatrix} =$$
$$\left\langle\ 1 - \prod_{j=1}^{|S_D|} \prod_{i=1}^{|S_A|} (1-\mu_{ij})^{p_i q_j},\quad \prod_{j=1}^{|S_D|} \prod_{i=1}^{|S_A|} {\nu_{ij}}^{p_i q_j}\ \right\rangle = \langle\mu,\nu\rangle \tag{30}$$

Since we are dealing with a zero-sum game, the equilibrium payoff value for the defender can be defined as $-E(\sigma_A, \sigma_D)$.

5 Experiment

In our experiments, we consider both local and global networks. A local network (such as a railway network between cities in a province) often has a small network size N, meaning that the number of strategy profiles needed for decision makers to compute the Nash equilibrium is not large. In the experiment, we focus on the probability distributions over each node and the equilibrium payoff values to decision makers based on intuitionistic fuzzy theory. We also explore the degree of the decision makers' subjective preferences for specific strategies. A global network often has a larger network size N (such as an airline network with $N = 100$), and the total number of strategy profiles is then more than 10^{60} when $\theta_A = \theta_D = 1$, $\omega_A = \omega_D = 0$. In this case, the payoff matrix is too large to construct, let alone solve[15], and we therefore use the typical strategies in Section 3.2. In the experiment, we focus on the probability distributions over typical strategies and the equilibrium payoff values to decision makers based on intuitionistic fuzzy theory. The variation in the Nash equilibrium for typical decision-making strategies in an optimistic scenario is presented. In this paper, we report the results of experiments on a local network with 10 nodes and a global network with 300 nodes.

5.1 Local network experiment

5.1.1 Experiment setting

We carried out experiments on a local network with the topological structure shown in Fig. 4. In this network, decision makers are fully capable of considering all strategies and obtaining the mixed-strategy Nash equilibrium. From both the perspective of the support set in mathematics and the perspective of the simultaneous game in experiments[16], it can be proven that a mixed strategy is more efficient in the Nash equilibrium than the typical strategies (HS, LS, RS).

To investigate the effects of the cost coefficient parameter and minimum resource utilization rate on the number of optional strategies in the target network, we take the attacker as an example. We set $q_A = q_D = 0.8$ and $\omega_A \in [0.5, 1]$ to reflect the actual situation. The possible values of θ_A range from 1/16 to 1, which can be seen from analyzing the network in Fig. 4. The results are illustrated in Fig. 5.

From Fig. 5, we see that there are more available strategies when θ_A is moderate, and the number of available strategies gradually decreases as ω_A increases. Based on the principle of maximizing resource utilization while simulating a more typical scenario, we set the cost constraint parameters for both the attacker and defender in Fig. 5 to 0.75 and the minimum resource utilization rate to 0.9 for the following analysis. To consider the decision makers' preferences, we set the corresponding MF/NF to the size of the largest connected component ($m_H^{\text{acc}} = 0.35$, $n_H^{\text{acc}} = 0.2$, $m_H^{\text{rej}} = 0.35$, $n_H^{\text{rej}} = 0.1$), network efficiency ($m_H^{\text{acc}} = 0.5$, $n_H^{\text{acc}} = 0.3$, $m_H^{\text{rej}} = 0.5$, $n_H^{\text{rej}} = 0.15$), and clustering coefficient (t=2, $m_E^{\text{acc}} = 0.6$, $n_E^{\text{acc}} = 0.3$, $m_E^{\text{rej}} = 0.55$, $n_E^{\text{rej}} = 0.1$) in Fig. 6, respectively.

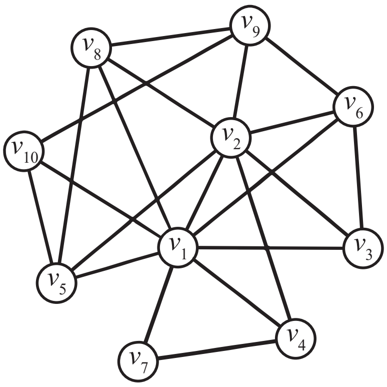
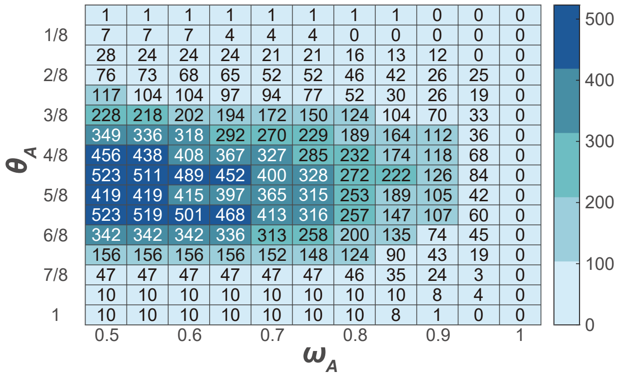


Fig. 4 Topological structure of the target network with 10 nodes and 21 edges.



	1	1	1	1	1	1	1	1	0	0	0
1/8	7	7	7	4	4	4	0	0	0	0	0
	28	24	24	24	21	21	16	13	12	0	0
2/8	76	73	68	65	52	52	46	42	26	25	0
	117	104	104	97	94	77	52	30	26	19	0
3/8	228	218	202	194	172	150	124	104	70	33	0
	349	336	318	292	270	229	189	164	112	36	0
4/8	456	438	408	367	327	285	232	174	118	68	0
	523	511	489	452	400	328	272	222	126	84	0
5/8	419	419	415	397	365	315	253	189	105	42	0
	523	519	501	468	413	316	257	147	107	60	0
6/8	342	342	342	336	313	258	200	135	74	45	0
	156	156	156	156	152	148	124	90	43	19	0
7/8	47	47	47	47	47	47	46	35	24	3	0
	10	10	10	10	10	10	10	10	8	4	0
1	10	10	10	10	10	10	10	8	1	0	0
	0.5		0.6		0.7		0.8		0.9		1

Fig. 5 Numbers of strategies under different constraints on θ_A and ω_A.

Finally, we set the relative weight of the constraints of MF/NF, denoted by λ, to 0.5.

5.1.2 Probability distributions over each node

We assign different weight proportions to the metrics, i.e., the size of the largest connected component, the network efficiency, and the clustering coefficient. By aggregating these metrics using Eq. (10), we can obtain different IFS payoff matrices. The solution process for the model presented in Section 4 allows us to calculate the mixed-strategy Nash equilibrium. To identify the nodes that are preferred by the attacker and the defender, we map the probabilities over pure strategies to those over each node in the following manner[16]:

$$\rho_A = \frac{1}{n_A}\sum_{i=1}^{m} p_i \cdot S_{A\tilde{i}} = \frac{1}{n_A}\sigma_A \cdot [S_{A1}, S_{A2}, \ldots, S_{Am}]^{\mathrm{T}} \tag{31}$$

$$\rho_D = \frac{1}{n_D}\sum_{j=1}^{n} q_j \cdot S_{D\tilde{j}} = \frac{1}{n_D}\sigma_D \cdot [S_{D1}, S_{D2}, \ldots, S_{Dn}]^{\mathrm{T}} \tag{32}$$

where $m = |S_A|$, $n = |S_D|$. $\rho_A = [\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_N]$ and $\rho_D = [\tilde{q}_1, \tilde{q}_2, \ldots, \tilde{q}_N]$ are the probability distributions over individual nodes of the attacker and the defender, respectively, and $\sigma_A = [p_1, p_2, \ldots, p_m]$ and $\sigma_D = [q_1, q_2, \ldots, q_n]$ are the probability distributions over all possible strategies for the two players.

We analyzed the probability distributions over nodes in games with payoffs of IFSs. Figure 7 present a comparison of the probability distributions over nodes before and after applying intuitionistic fuzzy theory for different weight allocations of the metrics. The relative weight of the constraints on MF/NF is set to 0.5 ($\lambda = 0.5$), and the size of each circle is proportional to the corresponding node degree.

When attacking or defending nodes, there are three factors that may affect the outcome: (1) the resources

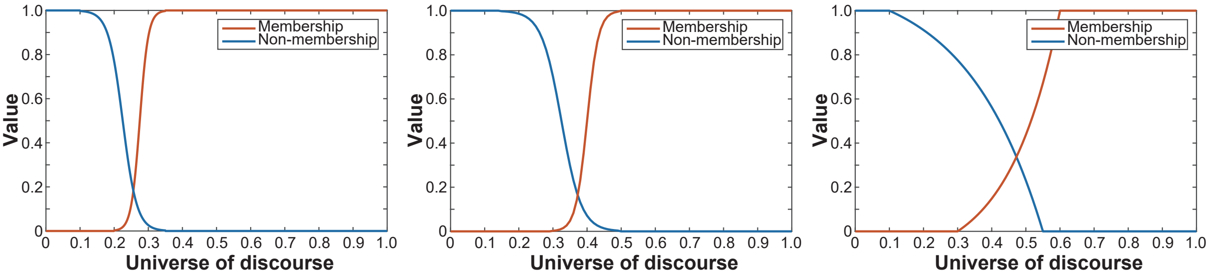


Fig. 6 Parameter setting of MF/NF when considerate different complex network metrics.

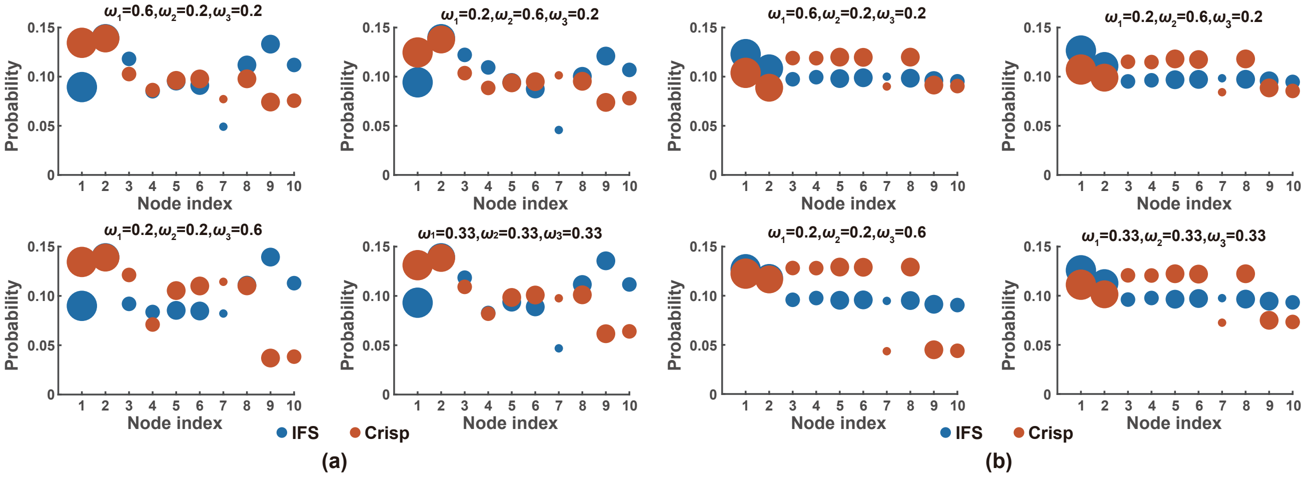


Fig. 7 Probabilities over each node of (a) the attacker and (b) the defender.

necessary for attacking or defending each node; (2) the individual preferences of the decision makers, as reflected by the MF/NF; and (3) the different weight proportions of the complex network metrics.

Figure 7a shows that under crisp conditions, the attacker is more inclined to attack nodes with higher importance; however, once intuitionistic fuzzy preferences are incorporated, the attacker becomes more sensitive to the necessary resources for attacking respective nodes, which elevates the likelihood of attacking moderately important nodes. Furthermore, our findings indicate that varying the weight proportions of the complex network metrics does not significantly modify the attacker's overall probability distribution for various nodes.

Figure 7b shows that under crisp conditions, the defender exhibits a greater inclination to protect moderately important nodes. Under intuitionistic fuzzy preferences, the defender's probability proportion for various nodes becomes more even, but a notable inclination toward protecting highly important nodes is seen. The defender believes that protecting nodes of greater importance could lead to an acceptable level of loss, from the perspective of a subjective judgment based on intuitionistic fuzzy theory. In addition, for different weight proportions of the complex network metrics, the defender's overall probability distribution for nodes exhibits minimal variation.

5.1.3 Changes in equilibrium payoff values for the local network

After aggregating the three complex network metrics with different weight proportions, we can obtain equilibrium payoff values for the attacker and defender using the method presented in Section 4. However, when we calculate the equilibrium payoff values in an IFS using Eq. (10), the resulting values are evidently inconsistent with reality. It can be observed that when one of the values of μ_{ij} equals one, the corresponding membership of the equilibrium payoff values also becomes one; likewise, if any of the values of ν_{ij} is zero, the corresponding non-membership of the equilibrium payoff values becomes zero. In order to avoid such a predicament, we replace the circumstance where $\mu_{ij}=1$ and $\nu_{ij}=0$ with an alternative setting where $\mu_{ij}=0.99$ and $\nu_{ij}=0.01$, respectively. Table 2 depicts the Nash equilibrium payoff values for the IFS

Table 2 Nash equilibrium payoff values in membership function and non-membership function degree.

Weight proportion	MF degree	NF degree
$\omega_1 = 0.6, \omega_2 = 0.2, \omega_2 = 0.2$	0.48	0.31
$\omega_1 = 0.2, \omega_2 = 0.6, \omega_2 = 0.2$	0.65	0.18
$\omega_1 = 0.2, \omega_2 = 0.2, \omega_2 = 0.6$	0.40	0.41
$\omega_1 = 0.33, \omega_2 = 0.33, \omega_2 = 0.33$	0.52	0.28

for differing weight proportions. The weights ω_1, ω_2, and ω_3 represent the size of the largest connected component, network efficiency, and clustering coefficient, respectively.

When network efficiency is emphasized, the Nash equilibrium payoff value for the attacker obtained under intuitionistic fuzzy conditions is maximal. When the size of the largest connected component is emphasized, the payoff value ranks second, and when the clustering coefficient is emphasized, the payoff value is minimal. As this is a zero-sum game, the defender's payoff values are precisely the converse of those of the attacker.

5.1.4 Impact of subjective judgement on strategies

Decision makers of different types tend to demonstrate varying degrees of subjective preference for certain strategies. We combine the methods described in Section 3.3 and introduce an optimistic MF/NF with a tolerance parameter ε to simulate the case where the attacker is particularly inclined to attack node 6 (i.e., the selected strategy includes node 6) when $\lambda = 0.5$, for example. Using the MF/NF in Fig. 6, combined with the expressions in Sections 2.4 and 2.5, we investigate the effect of varying ε for the NF from 0.05 to 0.2 on three equally weighted metrics. Even if both the attacker and defender choose strategies that include node 6, the degree of rejection in the IFS of payoffs as perceived by the attacker is not expected to be significantly high. Figure 8 was produced by applying the mapping method described in Eqs. (31) and (32).

The attack probability distribution for node 6 gradually rises as ε increases under the Nash equilibrium, when the attacker has a predisposition to attack node 6, which is consistent with the expected result.

In this case, we employ only an optimistic MF/NF for the attacker while keeping the payoff matrix unaltered for the defender. As a result, the mixed-strategy Nash equilibrium and probability distribution among various nodes remain consistent with previous scenarios from the defender's perspective.

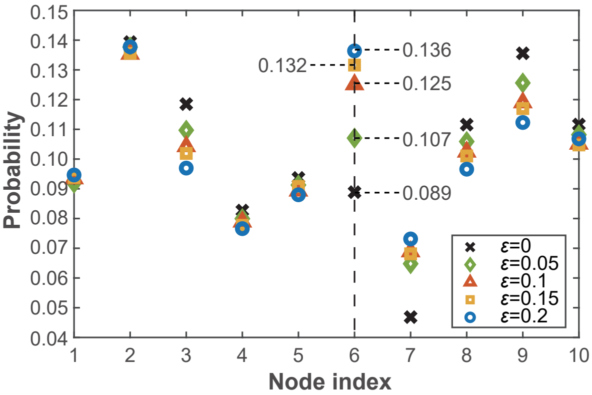


Fig. 8 Probabilities over each node of the attacker based on an intuitionistic fuzzy method.

5.2 Global network

5.2.1 Experiment setting

As scale-free networks with considerable numbers of nodes are widespread in the real world, we model the global network as a scale-free network with a power-law degree distribution ($p(k) \sim (\eta - 1)m^{\eta-1}k^{-\eta}$). We set $N = 300, \eta = 3$, and $m = 2$. For the MF/NF in the global network, we adopt the settings described in Section 5.1, whereby the relative weight of the constraints on the weight λ of the MF/NF is established as 0.5. Unlike the local network, we do not apply all the available strategies to the global network[54]; instead, we utilize the typical strategies (HS, LS, and RS) described in Section 3.2.

5.2.2 Nash equilibrium for the global network

First, we analyze the Nash equilibrium for the attacker and defender, assuming the same weight for the three metrics under crisp conditions, as shown in Fig. 9. The first and second rows show the probabilities adopted by the attacker and defender, respectively, while the first, second, and third columns show the results for HS, RS, and LS. The cost constraint parameters θ_A and θ_D reflect the different amounts of resources available to the attacker and defender, and range from 0.1 to 0.9. We also hypothesize an equiprobable weighting for the three complex network metrics. It seems that when the attacker has abundant resources (i.e., $\theta_A \in [0.8, 0.9]$), his probability of adopting RS is high. Conversely, when the attacker has limited resources (i.e., $\theta_A \in [0.1, 0.7]$), his probability of adopting LS is high. When both the attacker and defender have limited resources (i.e., $\theta_A \in [0.1, 0.5], \theta_D \in [0.1, 0.5]$), the defender is more likely to adopt HS or LS. Otherwise, the defender is more likely to adopt RS. We then

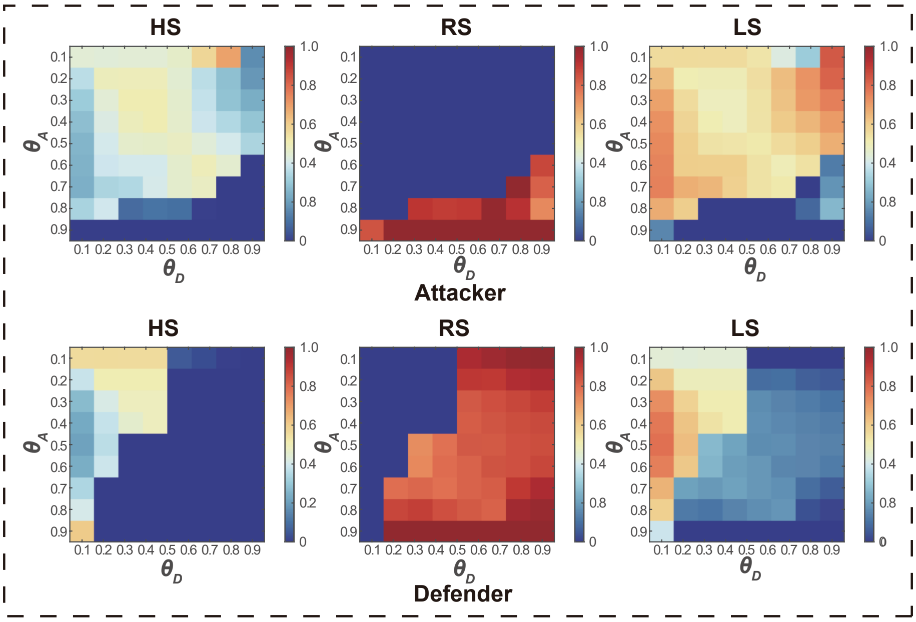


Fig. 9 Equilibrium strategies for the two players under crisp conditions.

examine the Nash equilibrium under different combinations of θ_A and θ_D for the attacker and defender when intuitionistic fuzzy theory is applied, and consider the three typical strategies with different weights for the aggregated metrics. In Fig. 10, different weight proportions are assigned to the size of the largest connected component, the network efficiency, and the clustering coefficient in each subgraph. The mixed Nash equilibrium strategies of the attacker and defender are obtained for different weight proportions. The weights ω_1, ω_2, and ω_3 represent the size of the largest connected component, the network efficiency, and the clustering coefficient, respectively.

We observe from Fig. 10 that there are three notable traits:

(1) When the defender has limited resources and the attacker has abundant resources (i.e., $\theta_D \in [0.1,0.4]$, $\theta_A \in [0.8,0.9]$), the attacker is likely to choose RS for all weight proportions.

(2) When both the attacker and defender have abundant resources (i.e., $\theta_A \in [0.6,0.9]$, $\theta_D \in [0.8,0.9]$), the attacker prefers LS for all weight proportions.

(3) For the defender, there is generally a higher probability of selecting RS for most combinations of θ_A and θ_D, particularly when the clustering coefficient weight is higher.

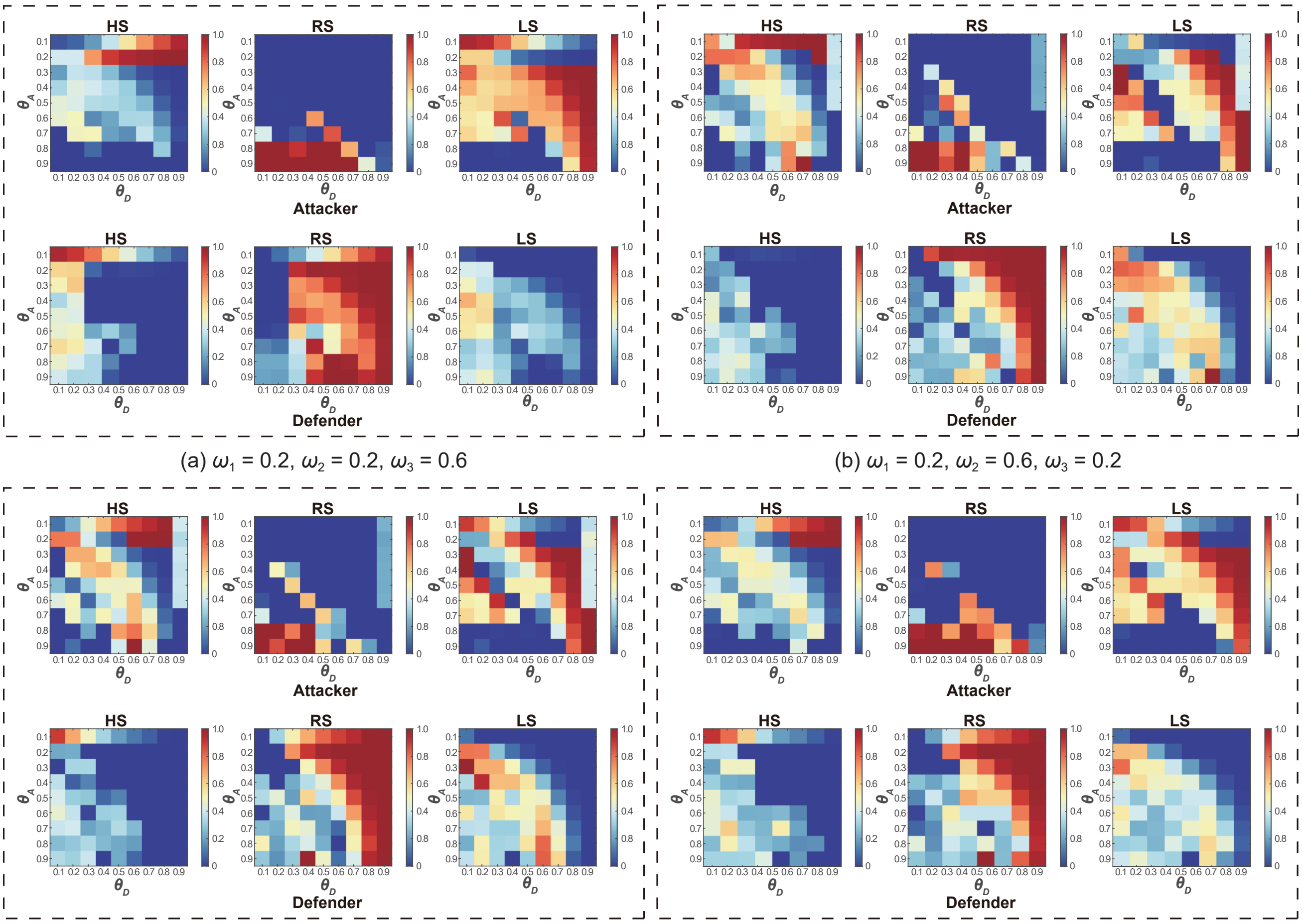
By combining Figs. 9 and 10d, we see that the Nash equilibrium for both the attacker and defender is impacted by the application of an intuitionistic fuzzy method as compared to the crisp situation.

For the attacker, when the defender has abundant resources but the attacker has limited resources (i.e., $\theta_D \in [0.6,0.9], \theta_A \in [0.1,0.2]$), the tendency of the attacker to adopt HS is significantly increased. When both the attacker and defender have abundant resources (i.e., $\theta_A \in [0.6,0.9], \theta_D \in [0.8,0.9]$), the tendency of the attacker to adopt LS is significantly increased.

For the defender, when the defender's available resources are moderate and the attacker's resources are rich ($\theta_D \in [0.2,0.7], \theta_A \in [0.6,0.9]$), the tendency for the defender to adopt RS is significantly decreased, while the tendency to adopt HS or LS is increased.

5.2.3 Changes in the equilibrium payoff value for the global network

Figure 11 displays the changes in the equilibrium intuitionistic fuzzy payoff value for the attacker when θ_A and θ_D vary within the interval $[0.1,0.9]$. Equations (26) and (27) show that the defender's equilibrium payoff value is the inverse of the attacker's, meaning that it is sufficient to analyze only the equilibrium payoff value for the attacker. The weights assigned to the metrics in Fig. 11 are derived from the corresponding weights presented in Fig. 10. The equilibrium payoff values for a game based on IFSs can be illustrated using two scales, relating to membership and non-membership values. In Fig. 11, these two scales are shown in yellow and green, respectively.



(a) ω_1 = 0.2, ω_2 = 0.2, ω_3 = 0.6

(b) ω_1 = 0.2, ω_2 = 0.6, ω_3 = 0.2

(c) ω_1 = 0.6, ω_2 = 0.2, ω_3 = 0.2

(d) ω_1 = 0.33, ω_2 = 0.33, ω_3 = 0.33

Fig. 10 Equilibrium strategies for the two players based on intuitionistic fuzzy theory.

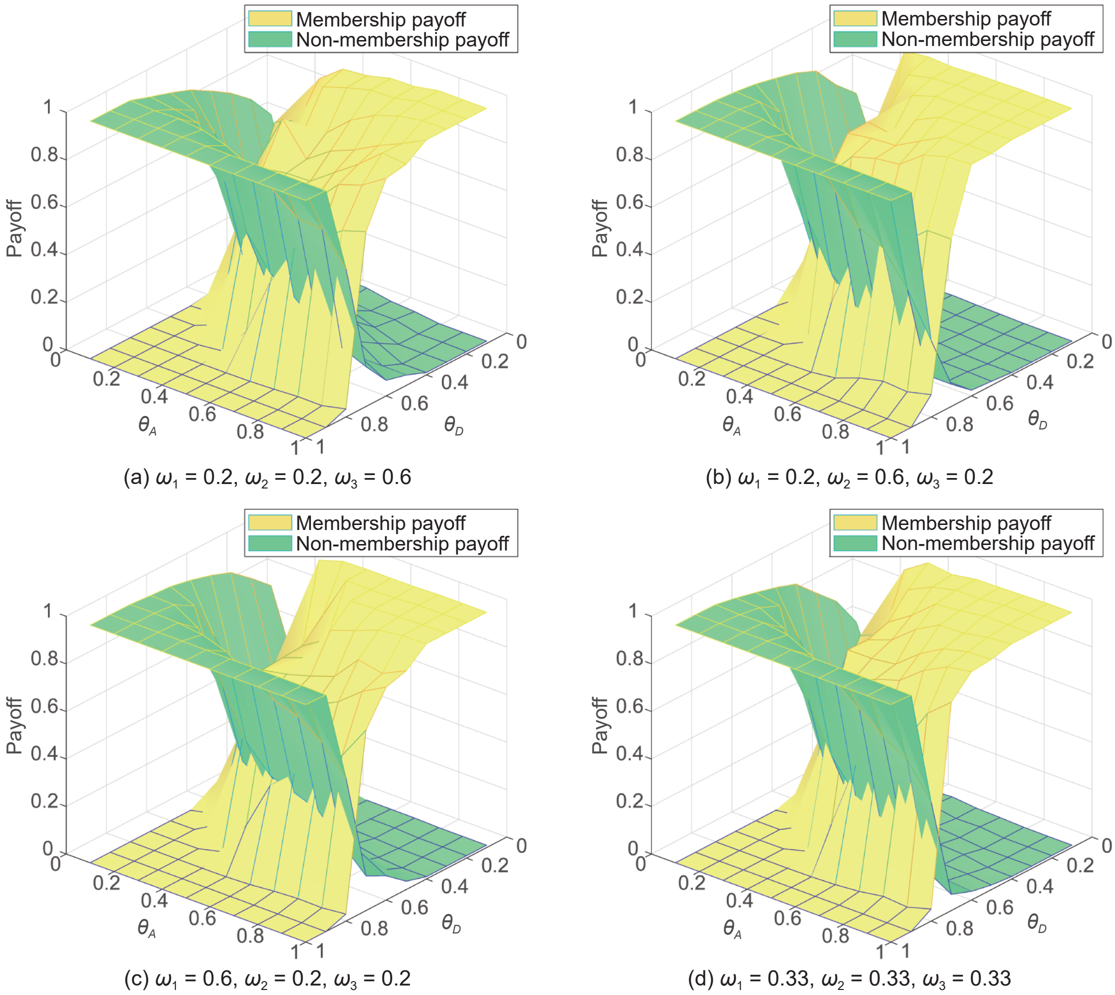
In general, the trends in the membership and non-membership equilibrium payoff values of the attacker stay consistent when the weight proportions of the metrics are varied. Despite minor changes in the value of the attacker’s equilibrium payoff across the four subplots for different combinations of θ_A and θ_D, two distinct features can be observed from all of the subplots:

(1) In Fig. 11, the change in the membership equilibrium payoff value is relatively smooth when it approaches one or zero. However, around 0.5, the value changes rapidly. This phenomenon can be attributed to the MF presented in Fig. 6. With this MF, when the payoff based on the metrics of the size of the largest connected component and network efficiency is moderately valued, the attacker’s marginal payoff increases significantly. As a result, the attacker tends to increase the payoff. Conversely, when the payoff is high, the attacker has mostly achieved the expected objectives, so the inclination to further increase the payoff is not strong. The non-membership equilibrium payoff value exhibits the same pattern.

(2) Figure 11 illustrates that when the attacker has abundant resources while the defender has few, the attacker’s equilibrium payoff value achieves the highest degree of membership and the lowest degree of non-membership. Conversely, when the attacker has limited resources but the defender has plenty, the situation is reversed, which is intuitively obvious. Regardless of the abundance of the attacker’s resources, when the defender has adequate resources, the equilibrium payoff for the attacker is the lowest. Meanwhile, as θ_D decreases for each fixed θ_A, the degree of membership in the equilibrium payoff for the attacker increases while the degree of non-membership decreases.

5.2.4 Impact of subjective judgment on typical strategies

In an actual game of attack and defense in infrastructure networks, decision makers of different



(a) ω_1 = 0.2, ω_2 = 0.2, ω_3 = 0.6

(b) ω_1 = 0.2, ω_2 = 0.6, ω_3 = 0.2

(c) ω_1 = 0.6, ω_2 = 0.2, ω_3 = 0.2

(d) ω_1 = 0.33, ω_2 = 0.33, ω_3 = 0.33

Fig. 11 Equilibrium payoff value of the attacker under different combinations of θ_A and θ_D.

types tend to demonstrate varying degrees of subjective preference for certain typical strategies. Using the method in Section 3.3, we introduce an optimistic approach to simulate the situation where the attacker is more inclined towards HS. The tolerance parameters for the optimistic MF/NF are set in the same way as in Fig. 8. Even if both the attacker and defender choose RS, the attacker does not perceive a high level of rejection in the rejection degree in the IFS of payoffs, which reflects the attacker's preference for RS. Figure 12 shows the increase in the attacker's probability of choosing HS under Nash equilibrium, with the tolerance ε varying from 0.05 to 0.2. This is calculated by subtracting the new probability of choosing RS from the original one, taking into account the attacker's various tolerance parameter settings.

From the results presented in Fig. 12, two observations can be made:

(1) Overall, the attacker has a higher probability of choosing RS when optimistic preferences are taken into consideration. This increase is particularly noticeable for certain combinations of θ_A and θ_D.

(2) For a combination of three metrics with equal weights, it is noticeable that the overall probability of choosing RS increases as the tolerance parameter setting rises. This trend can be observed from the magnitude of increase in the probability.

These results demonstrate the effectiveness of applying intuitionistic fuzzy MFs/NFs to describe the subjective preferences of different types of decision makers in game strategies.

6 Conclusion

In this paper, we use intuitionistic fuzzy theory to develop a feasible method of explaining the fuzziness of the payoffs in attack and defense games. We conduct experiments on both local and global networks, where we study the Nash equilibrium,

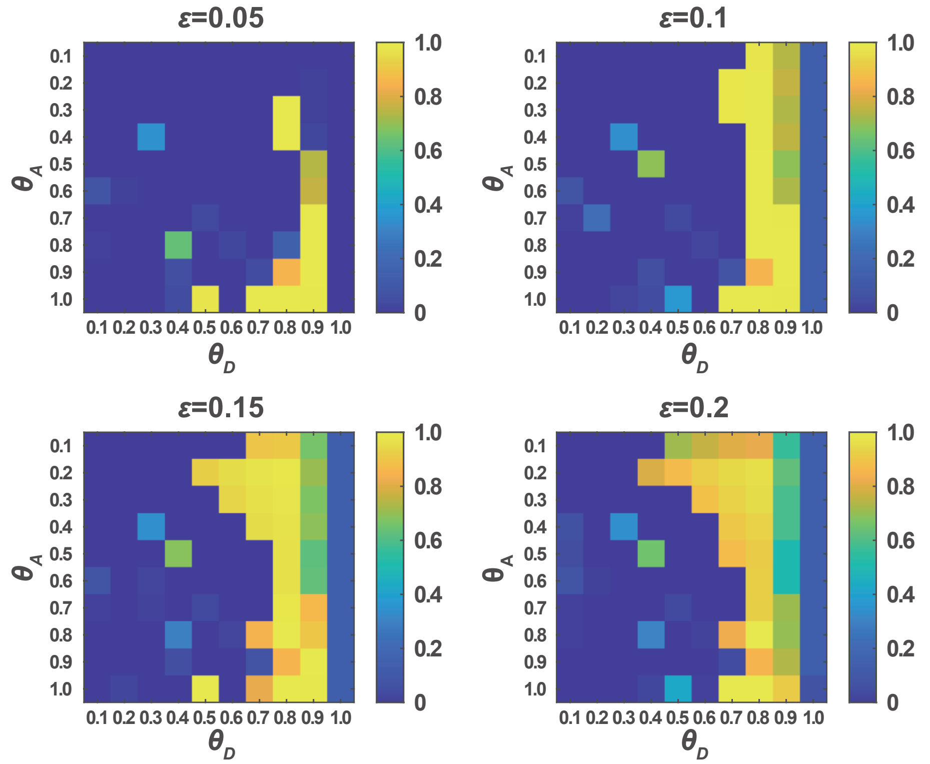


Fig. 12 The changes in the probability of RS under different combinations of θ_A and θ_D.

equilibrium payoff values and the impact of subjective judgment.

First, we construct the attack and defense game model based on intuitionistic fuzzy theory. For local and global networks, we propose two different strategy selection approaches. To assess the IFS payoffs in this model, we apply three distinct complex network metrics and design MFs/NFs base on the decision makers' subjective preferences. Second, we propose an algorithm to obtain the IFS payoff matrix. We then introduce a pair of nonlinear programming models to obtain the Nash equilibrium in a IFS zero-sum game for the attacker and defender. The attacker and defender's IFS equilibrium payoff values are also defined. Finally, to represent the network performance more comprehensively, we combine the payoff matrices obtained from the three metrics based on their respective weights, as per practical considerations. Our experimental results show that incorporating intuitionistic fuzzy theory lead to different Nash equilibrium values compared to crisp situations, and the equilibrium payoff values have some distinct features. In addition, differences in emphasis on the complex network metrics are not shown to affect the node probability distributions and Nash equilibria. Moreover, different tolerance parameters are found to have varying degrees of influence on the decision makers' equilibrium strategies.

References

[1] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, Energy-theft detection issues for advanced metering infrastructure in smart grid, *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105–120, 2014.

[2] R. Albert, H. Jeong, and A. L. Barabási, Error and attack tolerance of complex networks, *Nature*, vol. 406, pp. 378–382, 2000.

[3] F. Morone and H. A. Makse, Influence maximization in complex networks through optimal percolation, *Nature*, vol. 524, no. 7563, pp. 65–68, 2015.

[4] Z. G. Wang, Y. Deng, Z. Wang, and J. Wu, Disintegrating spatial networks based on region centrality, *Chaos*, vol. 31, no. 6, p. 061101, 2021.

[5] J. Hao, J. Yin, and B. Zhang, Structural fault tolerance of scale-free networks, *Tsinghua Science and Technology*, vol. 12, no. S1, pp. 246–249, 2007.

[6] N. Fan and P. M. Pardalos, Robust optimization of graph partitioning and critical node detection in analyzing networks, in *Proc. 4th Int. Conf. Combinatorial optimization and applications - Volume Part I*, Kailua-Kona, HI, USA, 2010, pp. 170–183.

[7] B. Addis, R. Aringhieri, A. Grosso, and P. Hosteins, Hybrid constructive heuristics for the critical node problem, *Ann. Oper. Res.*, vol. 238, no. 1, pp. 637–649,

2016.

[8] M. Bernaschi, A. Celestini, M. Cianfriglia, S. Guarino, G. F. Italiano, E. Mastrostefano, and L. R. Zastrow, Seeking critical nodes in digraphs, *J. Comput. Sci.*, vol. 69, p. 102012, 2023.

[9] J. V. Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton, NJ, USA: Princeton University, 1953.

[10] J. F. Nash, Equilibrium points in N-person games, *Proc. Natl. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, 1950.

[11] X. Song, W. Jiang, X. Liu, H. Lu, Z. Tian, and X. Du, A survey of game theory as applied to social networks, *Tsinghua Science and Technology*, vol. 25, no. 6, pp. 734–742, 2020.

[12] G. G. Brown, W. M. Carlyle, J. Salmerón, and K. Wood, Analyzing the vulnerability of critical infrastructure to attack and planning defenses, *Emerging Theory, Methods, and Applications*, pp. 102–123, 2005.

[13] G. G. Brown and L. A. T. Cox Jr, How probabilistic risk assessment can mislead terrorism risk analysts, *Risk Anal.*, vol. 31, no. 2, pp. 196–204, 2011.

[14] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, Defending critical infrastructure, *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.

[15] Y. P. Li, S. Y. Tan, Y. Deng, and J. Wu, Attacker-defender game from a network science perspective, *Chaos*, vol. 28, no. 5, p. 051102, 2018.

[16] Y. Li, Y. Xiao, Y. Li, and J. Wu, Which targets to protect in critical infrastructures - A game-theoretic solution from a network science perspective, *IEEE Access*, vol. 6, pp. 56214–56221, 2018.

[17] Y. Li, Y. Deng, Y. Xiao, and J. Wu, Attack and defense strategies in complex networks based on game theory, *J. Syst. Sci. Complex.*, vol. 32, no. 6, pp. 1630–1640, 2019.

[18] C. Fu, Y. Gao, J. Zhong, Y. Sun, P. Zhang, and T. Wu, Attack-defense game for critical infrastructure considering the cascade effect, *Reliab. Eng. Syst. Saf.*, vol. 216, p. 107958, 2021.

[19] C. Fu, P. Zhang, L. Zhou, Y. Gao, and N. Du, Camouflage strategy of a Stackelberg game based on evolution rules, *Chaos Solitons Fractals*, vol. 153, p. 111603, 2021.

[20] X. Gu, C. Zeng, and F. Xiang, Applying a Bayesian Stackelberg game to secure infrastructure system: From a complex network perspective, in *Proc. 2019 4th Int. Conf. Automation, Control and Robotics Engineering*, Shenzhen, China, 2019, pp. 1–6.

[21] C. Zeng, B. Ren, M. Li, H. Liu, and J. Chen, Stackelberg game under asymmetric information in critical infrastructure system: From a complex network perspective, *Chaos*, vol. 29, no. 8, p. 083129, 2019.

[22] C. Zeng, B. Ren, H. Liu, and J. Chen, Applying the Bayesian stackelberg active deception game for securing infrastructure networks, *Entropy*, vol. 21, no. 9, p. 909, 2019.

[23] K. H. Thompson and H. T. Tran, Application of a defender-attacker-defender model to the U.S. air transportation network, in *Proc. IEEE Int. Symp. on Technologies for Homeland Security* (*HST*), Woburn, MA, USA, 2018, pp.1–5.

[24] K. H. Thompson and H. T. Tran, Operational perspectives into the resilience of the U.S. air transportation network against intelligent attacks, *IEEE Trans. Intell. Transport. Syst.*, vol. 21, no. 4, pp. 1503–1513, 2020.

[25] G. Qi, J. Li, X. Xu, G. Chen, and K. Yang, An attack-defense game model in infrastructure networks under link hiding, *Chaos Interdiscip. J. Nonlinear Sci.*, doi: 10.1063/5.0112907.

[26] G. Qi, J. Li, C. Xu, G. Chen, and K. Yang, Attack-defense game model with multi-type attackers considering information dilemma, *Entropy*, vol. 25, no. 1, p. 57, 2022.

[27] Y. Huang, J. Wu, C. K. Tse, and Z. Zheng, Sequential attacker-defender game on complex networks considering the cascading failure process, *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 2, pp. 518–529, 2022.

[28] J. Tan, H. Jin, H. Hu, R. Hu, H. Zhang, and H. Zhang, WF-MTD: Evolutionary decision method for moving target defense based on wright-fisher process, *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 4719–4732, 2023.

[29] H. Zhang, Y. Mi, X. Liu, Y. Zhang, J. Wang, and J. Tan, A differential game approach for real-time security defense decision in scale-free networks, *Comput. Netw.*, vol. 224, p. 109635, 2023.

[30] H. Zhang, Y. Mi, Y. Fu, X. Liu, Y. Zhang, J. Wang, and J. Tan, Security defense decision method based on potential differential game for complex networks, *Comput. Secur.*, vol. 129, p. 103187, 2023.

[31] L. A. Zadeh, Fuzzy sets, *Inf. Contr.*, vol. 8, no. 3, pp. 338–353, 1965.

[32] K. T. Atanassov, Intuitionistic fuzzy sets, *Fuzzy Sets Syst.*, vol. 20, no. 1, pp. 87–96, 1986.

[33] K. T. Atanassov, Research on intuitionistic fuzzy sets in Bulgaria, *Fuzzy Sets Syst.*, vol. 22, no. 1&2, p. 193, 1987.

[34] F. Xiao, A distance measure for intuitionistic fuzzy sets and its application to pattern classification problems, *IEEE Trans. Syst. Man Cybern, Syst.*, vol. 51, no. 6, pp. 3980–3992, 2021.

[35] D. Xie, F. Xiao, and W. Pedrycz, Information quality for intuitionistic fuzzy values with its application in decision making, *Eng. Appl. Artif. Intell.*, vol. 109, p. 104568, 2022.

[36] Y. Fan and F. Xiao, TDIFS: Two dimensional intuitionistic fuzzy sets, *Eng. Appl. Artif. Intell.*, vol. 95, p. 103882, 2020.

[37] K. T. Atanassov, *Intuitionistic Fuzzy Sets Theory and Applications*. Heidelberg, Germany: Physica-Heidelberg, 1999.

[38] K. T. Atanassov, My personal view on intuitionistic fuzzy sets theory, in *Fuzzy Sets and Their Extensions*: *Representation, Aggregation and Models*, H. Bustince, F. Herrera, and J. Montero, eds. Berlin, Heidelberg: Springer, 2008, pp. 23–43.

[39] P. P. Angelov, Optimization in an intuitionistic fuzzy environment, *Fuzzy Sets Syst.*, vol. 86, no. 3, pp. 299–306, 1997.

[40] D. Dubey, S. Chandra, and A. Mehra, Fuzzy linear programming under interval uncertainty based on IFS representation, *Fuzzy Sets Syst.*, vol. 188, no. 1, pp. 68–87,

2012.

[41] D. Rani, T. R. Gulati, and H. Garg, Multi-objective non-linear programming problem in intuitionistic fuzzy environment: Optimistic and pessimistic view point, *Expert Syst. Appl.*, vol. 64, pp. 228–238, 2016.

[42] S. K. Singh and S. P. Yadav, Intuitionistic fuzzy multi-objective linear programming problem with various membership functions, *Ann. Oper. Res.*, vol. 269, no. 1, pp. 693–707, 2018.

[43] I. P. Debnath and S. K. Gupta, Exponential membership function and duality gaps for I-fuzzy linear programming problems, *Iran. J. Fuzzy. Syst.*, vol. 16, no. 2, pp. 147–163, 2019.

[44] R. Cohen and S. Havlin, *Complex Networks*. Cambridge, UK: Cambridge University Press, 2010.

[45] V. Latora and M. Marchiori, Efficient behavior of small-world networks, *Phys. Rev. Lett.*, vol. 87, no. 19, p. 198701, 2001.

[46] D. J. Watts and S. H. Strogatz, Collective dynamics of ‘small-world’ networks, *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[47] B. Jana and T. K. Roy, Multi-objective intuitionistic fuzzy linear programming and its application in transportation model, *Notes. Intuit. Fuzzy. Sets.*, vol. 13, p. 1, 2007.

[48] R. Verma, M. P. Biswal, and A. Biswas, Fuzzy programming technique to solve multi-objective transportation problems with some non-linear membership functions, *Fuzzy Sets Syst.*, vol. 91, no. 1, pp. 37–43, 1997.

[49] S. Mahajan and S. K. Gupta, On optimistic, pessimistic and mixed approaches under different membership functions for fully intuitionistic fuzzy multiobjective nonlinear programming problems, *Expert Syst. Appl.*, vol. 168, p. 114309, 2021.

[50] H. Bustince and P. Burillo, Structures on intuitionistic fuzzy relations, *Fuzzy Sets Syst.*, vol. 78, no. 3, pp. 293–303, 1996.

[51] Z. Xu, A deviation-based approach to intuitionistic fuzzy multiple attribute group decision making, *Group Decis. Negot.*, vol. 19, no. 1, pp. 57–76, 2010.

[52] D. Hernández Serrano and D. Sánchez Gómez, Centrality measures in simplicial complexes: Applications of topological data analysis to network science, *Appl. Math. Comput.*, vol. 382, p. 125331, 2020.

[53] D. F. Li and J. X. Nan, A nonlinear programming approach to matrix games with payoffs of atanassov’s intuitionistic fuzzy sets, *Int. J. Uncertain.*, doi: 10.1142/S0218488509006157.

[54] T. Basar, G. J. Olsder, *Dynamic Noncooperative Game Theory*. Philadelphia, PA, USA: SIAM Press, 1999.

Jiaqi Ren received the BS degree in business school from Northeast Normal University, Changsha, China, in 2023. She is currently pursuing the MS degree in management science and engineering from National University of Defense Technology, Changsha, China. Her current research interests include game theory and complex network.

Zhe Li received the BS degree in operation research and mission planning from National University of Defense Technology, Changsha, China, in 2023. He is currently pursuing the MS degree in management science and engineering from National University of Defense Technology, Changsha, China. His current research interests include attack and defense game and multilayer network.

Weili Li received the BS and PhD degrees in system engineering from National University of Defense Technology, Changsha, China, in 2012 and 2019, respectively. She is currently an associate professor with Department of System Engineering, National University of Defense Technology. Her current research interests include security game and complex network.

Yibo Dong received the BS degree in management science and engineering from National University of Defense Technology, Changsha, China, in 2022. He is currently pursuing the MS degree in management science and engineering from National University of Defense Technology, Changsha, China. His current research interests include fuzzy game, security game, and complex network.

Jin Liu received the BS, MS, and PhD degrees in mathematics from Tsinghua University, Beijing, China, in 2005, 2008, and 2011, respectively. He has been an assistant professor from 2011–2017, an associate professor from 2017 to 2023, and a full professor from 2023 to present with National Key Laboratory of Information Systems Engineering, National University of Defense Technology, Changsha, China. His current research interests include fuzzy systems, uncertain systems, and their applications in game theory, optimization theory, and artificial intelligence. He has authored or coauthored over 100 articles written in Chinese or English and 15 academic books written in Chinese.