*mathematics*

MDPI

*Article*

# Protecting Infrastructure Networks: Solving the Stackelberg Game with Interval-Valued Intuitionistic Fuzzy Number Payoffs

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

Science and Technology on Information Systems Engineering Laboratory, National University of Defense Technology, Changsha 410073, China; dongyibo@nudt.edu.cn (Y.D.); liujin229234@nudt.edu.cn (J.L.); jiaqiren@nudt.edu.cn (J.R.); lizhe@nudt.edu.cn (Z.L.)
* Correspondence: weiwei6563@nudt.edu.cn

**Abstract:** Critical infrastructure is essential for the stability and development of modern society, and a combination of complex network theory and game theory has become a new research direction in the field of infrastructure protection. However, existing studies do not consider the fuzziness and subjective factors of human judgment, leading to challenges when analyzing strategic interactions between decision makers. This paper employs interval-valued intuitionistic fuzzy numbers (IVIFN) to depict the uncertain payoffs in a Stackelberg game of infrastructure networks and then proposes an algorithm to solve it. First, we construct IVIFN payoffs by considering the different complex network metrics and subjective preferences of decision makers. Next, we propose a lexicographic algorithm to solve this game based on the concept of a strong Stackelberg equilibrium (SSE). Finally, we conduct experiments on target scale-free networks. Our results illustrate that in an SSE, for the defender in a weak position, it is better to defend nodes with high degrees. The experiments also indicate that taking fuzziness into account leads to higher SSE payoffs for the defender. Our work aims to solve a Stackelberg game with IVIFN payoffs and apply it to enhance the protection of infrastructure networks, thereby improving their overall security.

**Keywords:** infrastructure networks; Stackelberg game; interval-valued intuitionistic fuzzy theory; strong Stackelberg equilibrium

**MSC:** 91A86



**Citation:** Dong, Y.; Liu, J.; Ren, J.; Li, Z.; Li, W. Protecting Infrastructure Networks: Solving the Stackelberg Game with Interval-Valued Intuitionistic Fuzzy Number Payoffs. *Mathematics* **2023**, *11*, 4992. https://doi.org/10.3390/math11244992

Academic Editors: Jun Ye and Yanhui Guo

Received: 16 November 2023
Revised: 11 December 2023
Accepted: 12 December 2023
Published: 18 December 2023



## 1. Introduction

Critical infrastructures, such as power grids, transportation systems, communication networks, and water supply networks, play vital roles in modern society. On 7 October 2023, Hamas launched an attack on Israel, utilizing drones to target and destroy communications equipment at surveillance posts along the borders of the Gaza Strip. In response, Israel launched thousands of missiles to destroy Gaza's cables, cell towers, and infrastructure needed to keep people online. Therefore, the protection of critical infrastructure networks has become increasingly challenging and deserves further study. Probabilistic risk assessment (PRA) is a conventional and commonly used method for the analysis of infrastructure investment and protection [1,2]. However, such analysis is resource-intensive and quickly becomes complex, even for small systems. Complex network theory has emerged as a novel approach to overcome the limitations of PRA in dealing with the protection of infrastructure systems. Lee and Tien [3] investigated the impact of variations in three parameters of network vulnerability, namely component vulnerabilities, service interdependency redundancies, and system link configurations. Liu et al. [4] investigated interdependent critical infrastructure networks and designed a cascading failure model, examining cascading failure in both syncretic and single networks. Herrera et al. [5] presented a multilayer complex network framework taking into account the heterogeneity of the redundant infrastructure for realistic network modeling. Recent studies have been

conducted on complex networks such as network disintegration [6–8] and protection [9–11]. These studies have provided effective ways to obtain insights into network attacks and to identify the systems and components that must be protected.

To deal with deliberate attacks, the combination of network science and game theory has garnered considerable research attention. Li et al. [12] applied a simultaneous game and defined payoffs according to the topology of the infrastructure system. They then considered two typical strategies under a cost constraint model [13]. Fu et al. [14] proposed a static network attack and defense game model to examine the impact of cascading failures. Sun et al. [15] established a network attack and defense game model based on betweenness virtual flow. Although a simultaneous game is an important game model, Stackelberg games are more commonly used to model attack and defense scenarios in security domains, as they align better with real-life situations [16]. Li et al. [17] applied a Stackelberg game model to complex networks and evaluated the effects of cost-sensitive parameters. Zeng et al. [18,19] proposed a false network construction method and applied Stackelberg and Bayesian Stackelberg game models for the defense of critical infrastructure networks. Fu et al. [20] established a Stackelberg game model based on camouflage strategies and proposed an evolutionary rule to optimize these strategies. Qi et al. [21,22] 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. Liu et al. [23] established an attack-defensive game model based on a Stackelberg game under asymmetric information, obtaining a defensive resource allocation strategy to optimize the network robustness. Liu et al. [24] established a Stackelberg game model based on a 5G network graph and proposed compact particle swarm optimization based on the location-scale distribution to solve the Nash equilibrium.

However, the aforementioned research fails to consider the problem in a fuzzy environment. The topology of real-world infrastructure networks exhibits numerous features; even if the same nodes are removed after an attack, the effects of the attack can vary when measured using different network metrics [25,26]. Hence, the assessment of an attack's impact (i.e., the payoffs for both the attacker and the defender) naturally contains fuzziness and uncertainty. In addition, subjective factors and human judgment are challenges in the analysis of the strategic interactions between decision makers. Fuzzy set theory, proposed by Zadeh [27] in 1965, provides a preliminary tool to handle these problems. Atanassov extended the notion of fuzzy sets to intuitionistic fuzzy sets by appending a degree of nonmembership [28,29]. Unfortunately, for attack and defense games in infrastructure networks, it may be difficult to identify exact values for the membership and nonmembership degrees of impact after a confrontation. Thus, the payoffs of the game seem to be suitably expressed with interval-valued intuitionistic fuzzy numbers (IVIFN) [30]. The IVIFN is characterized by introducing the degrees of membership and nonmembership as whole intervals instead of crisp values. As is known, IVIFN has been extensively applied in the field of decision making [31–37], and the research in this field has provided several useful methodologies. Many studies have focused on solving the simultaneous game with IVIFN payoffs. Li [38] proved that matrix games with interval-valued intuitionistic fuzzy set (IVIFS) payoffs have solutions, and he developed a mathematical programming methodology by constructing a pair of auxiliary linear/nonlinear programming models to solve these games. Xia [39] proposed several mathematical programming models to find solutions of IVIFN matrix games based on Archimedean t-conorm and t-norm and transformed them into a pair of primal–dual linear programming models. Kumar et al. [40] developed a solution for a two-person zero-sum game with IVIFN payoffs by introducing a new order function to defuzzify the IVIFNs. Naqvi et al. [41] extended the work of Li [38] by proposing a solution for a matrix game with payoffs characterized by linguistic IVIFSs.

To the best of our knowledge, no existing literature has delved into the modeling of fuzzy payoffs for the game in infrastructure networks. Moreover, to the best of our knowledge, no existing research has studied a method to solve Stackelberg games in an interval-valued intuitionistic fuzzy (IVIF) environment. These limitations highlight the

need for further research in the area of infrastructure protection. In this paper, we evaluate attack and defense performance using various complex network metrics and introduce a method of constructing them as IVIFNs. Furthermore, we establish a Stackelberg game with IVIFN payoffs where the defender (leader) commits to a strategy before the attacker (follower) selects its own strategy. Inspired by the work of Conitzer et al. [42], we propose a lexicographic method to solve this game. In this method, we use score and accuracy functions to consider the risk attitude of the decision maker by defining two comparison indices arranged in a hierarchical fashion [34]. We then conduct experiments under different available resources and risk attitudes of both the attacker and the defender. We analyze the results of the experiment using a scale-free network as the target. Overall, the model and solution method proposed in this paper enable the incorporation of more payoff information, accounting for factors such as fuzziness, uncertainty, and decision makers' subjective preferences in the context of protecting infrastructure networks. This extension enhances the applicability of the game model to real-world scenarios and offers a more rational basis for strategy selection. Furthermore, this research provides insights that can inform defenders in the protection of infrastructure networks.

## 2. Preliminaries

In this section, we briefly review the basic concepts of IVIFSs and IVIFNs and the different ranking methods of the latter. We also review a classical Stackelberg game (one attacker and one defender) and its SSE.

### *2.1. Regarding the IVIF Theory*

**Definition 1.** *An IVIFS $\tilde{A}$ in the universe of discourse $Z$ is defined by [30]* $\tilde{A} = \left\{ \left\langle x, \left[\mu_{\tilde{A}}^{L}(x), \mu_{\tilde{A}}^{U}(x)\right], \left[\nu_{\tilde{A}}^{L}(x), \nu_{\tilde{A}}^{U}(x)\right] \right\rangle \mid x \in Z \right\}$, *where* $\left[\mu_{\tilde{A}}^{L}(x), \mu_{\tilde{A}}^{U}(x)\right] \in D[0,1]$ *and* $\left[\nu_{\tilde{A}}^{L}(x), \nu_{\tilde{A}}^{U}(x)\right] \in D[0,1]$, *with the condition* $0 \leq \mu_{\tilde{A}}^{U}(x) + \nu_{\tilde{A}}^{U}(x) \leq 1, \forall x \in Z$. *Here, the intervals* $\left[\mu_{\tilde{A}}^{L}(x), \mu_{\tilde{A}}^{U}(x)\right]$, *and* $\left[\nu_{\tilde{A}}^{L}(x), \nu_{\tilde{A}}^{U}(x)\right]$, *respectively, represent the membership degree and nonmembership degree of the element* $x \in Z$ *to* $\tilde{A}$. *For each element* $x$, *the hesitancy degree of* $x \in Z$ *to* $\tilde{A}$ *is defined as* $\left[1 - \mu_{\tilde{A}}^{U}(x) - \nu_{\tilde{A}}^{U}(x), 1 - \mu_{\tilde{A}}^{L}(x) - \nu_{\tilde{A}}^{L}(x)\right]$.

*In [31], Xu called the pair* $\langle [\mu^L, \mu^U], [\nu^L, \nu^U] \rangle$ *an IVIFN, where* $0 \leq \mu^L \leq \mu^U \leq 1$, $0 \leq \nu^L \leq \nu^U \leq 1$, *and* $0 \leq \mu^U + \nu^U \leq 1$.

**Definition 2.** *Let* $\tilde{\xi}_1 = \langle [\mu_1^L, \mu_1^U], [\nu_1^L, \nu_1^U] \rangle$ *and* $\tilde{\xi}_2 = \langle [\mu_2^L, \mu_2^U], [\nu_2^L, \nu_2^U] \rangle$ *be any two IVIFNs; then [30],*

*(1)* $\tilde{\xi}_1 \prec \tilde{\xi}_2 (\tilde{\xi}_1 < \tilde{\xi}_2)$ *iff* $\mu_1^L < \mu_2^L, \mu_1^U < \mu_2^U, \nu_1^L > \nu_2^L$ *and* $\nu_1^U > \nu_2^U$;
*(2)* $\tilde{\xi}_1 = \tilde{\xi}_2$ *iff* $\mu_1^L = \mu_2^L, \mu_1^U = \mu_2^U, \nu_1^L = \nu_2^L$ *and* $\nu_1^U = \nu_2^U$;
*(3)* $\tilde{\xi}_1 + \tilde{\xi}_2 = \langle [\mu_1^L + \mu_2^L - \mu_1^L \mu_2^L, \mu_1^U + \mu_2^U - \mu_1^U \mu_2^U], [\nu_1^L \nu_2^L, \nu_1^U \nu_2^U] \rangle$;
*(4)* $\tilde{\xi}_1 \tilde{\xi}_2 = \langle [\mu_1^L \mu_2^L, \mu_1^U \mu_2^U], [\nu_1^L + \nu_2^L - \nu_1^L \nu_2^L, \nu_1^U + \nu_2^U - \nu_1^U \nu_2^U] \rangle$;
*(5)* $r\tilde{\xi}_1 = \left\langle \left[1 - \left(1 - \mu_1^L\right)^r, 1 - \left(1 - \mu_1^U\right)^r\right], \left[\left(\nu_1^L\right)^r, \left(\nu_1^U\right)^r\right] \right\rangle$.

**Definition 3.** *Xu's method of ranking IVIFNs is shown as follows [31]. For an IVIFN* $\tilde{\xi} = \langle [\mu^L, \mu^U], [\nu^L, \nu^U] \rangle$, *the score function XSF and accuracy function XAF of the IVIFN* $\tilde{\xi}$ *can be computed as*

$$XSF(\tilde{\xi}) = \frac{\mu^L + \mu^U - \nu^L - \nu^U}{2}, \tag{1}$$

$$XAF(\tilde{\xi}) = \frac{\mu^L + \mu^U + \nu^L + \nu^U}{2}, \tag{2}$$

*where* $-1 \leq XSF(\tilde{\xi}) \leq 1$ *and* $0 \leq XAF(\tilde{\xi}) \leq 1$.

*Let* $\tilde{\xi}_1$ *and* $\tilde{\xi}_2$ *be any two IVIFNs; then,*

*(1) If* $XSF(\tilde{\xi}_1) < XSF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 < \tilde{\xi}_2$;

(2) *If* $XSF(\tilde{\xi}_1) > XSF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 > \tilde{\xi}_2$;
(3) *If* $XSF(\tilde{\xi}_1) = XSF(\tilde{\xi}_2)$, *then*
  (i) *If* $XAF(\tilde{\xi}_1) < XAF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 < \tilde{\xi}_2$;
  (ii) *If* $XAF(\tilde{\xi}_1) > XAF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 > \tilde{\xi}_2$;
  (iii) *If* $XAF(\tilde{\xi}_1) = XAF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 = \tilde{\xi}_2$.

*However, Xu's method of ranking IVIFNs has the shortcoming that it cannot distinguish IVIFNs* $\langle [\mu_1^L, \mu_1^U], [\nu_1^L, \nu_1^U] \rangle$ *and* $\langle [\mu_2^L, \mu_2^U], [\nu_2^L, \nu_2^U] \rangle$ *if* $\mu_1^L + \mu_1^U = \mu_2^L + \mu_2^U$ *and* $\nu_1^L + \nu_1^U = \nu_2^L + \nu_2^U$.

**Definition 4.** *Wang and Wan's method of ranking IVIFNs is shown as follows [34]. For an IVIFN* $\tilde{\xi} = \langle [\mu^L, \mu^U], [\nu^L, \nu^U] \rangle$, *the score function WSF and accuracy function WAF of the IVIFN* $\tilde{\xi}$ *can be computed as*

$$WSF(\tilde{\xi}) = \lambda\left(\mu^L - \nu^U\right) + (1-\lambda)\left(\mu^U - \nu^L\right), \tag{3}$$

$$WAF(\tilde{\xi}) = \lambda\left(\mu^L + \nu^U\right) + (1-\lambda)\left(\mu^U + \nu^L\right), \tag{4}$$

*where* $-1 \le WSF(\tilde{\xi}) \le 1, 0 \le WAF(\tilde{\xi}) \le 1$, *and* $\lambda \in [0,1]$ *is the risk attitude parameter of the decision maker.*

*Let* $\tilde{\xi}_1$ *and* $\tilde{\xi}_2$ *be any two IVIFNs; then,*

(1) *If* $WSF(\tilde{\xi}_1) < WSF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 < \tilde{\xi}_2$;
(2) *If* $WSF(\tilde{\xi}_1) > WSF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 > \tilde{\xi}_2$;
(3) *If* $WSF(\tilde{\xi}_1) = \mathrm{WSF}(\tilde{\xi}_2)$, *then*
  (i) *If* $WAF(\tilde{\xi}_1) < WAF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 < \tilde{\xi}_2$;
  (ii) *If* $WAF(\tilde{\xi}_1) > WAF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 > \tilde{\xi}_2$;
  (iii) *If* $WAF(\tilde{\xi}_1) = WAF(\tilde{\xi}_2)$, *then* $\tilde{\xi}_1 = \tilde{\xi}_2$.

*In this ranking method, the decision maker is considered risk-seeking when* $\lambda \in [0, 0.5)$ *and risk-averse when* $\lambda \in (0.5, 1]$. *If* $\lambda = 0.5$, *the decision maker is neutral to risk, and Equations (3) and (4) are reduced to Equations (1) and (2). Therefore, Wang and Wan's ranking method is a general extension of Xu's ranking method.*

### 2.2. The Stackelberg Game

In a normal-form Stackelberg game, the defender is the leader and the attacker is the follower. $S_D$ and $S_A$ denote the strategy sets of the defender and the attacker. The payoff functions of the attacker and the defender can be represented as $f_A : S_D \times S_A \to \mathbb{R}$ and $f_D : S_D \times S_A \to \mathbb{R}$, respectively. The payoffs under different strategy profiles are real numbers. In this game, the attacker obtains the defender's mixed strategy and chooses the best response strategy. Correspondingly, the defender has the ability to anticipate the attacker's preferred strategy before committing to a mixed strategy. The Stackelberg game model is shown in Figure 1.

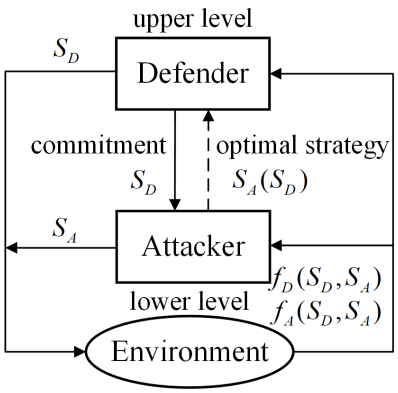



**Figure 1.** The framework of the Stackelberg game.

### *2.3. The Strong Stackelberg Equilibrium*

A Stackelberg equilibrium, which is the conceptual solution of Stackelberg games, captures the optimal outcome of the defender's strategy, since the attacker will always respond optimally to the defender's strategy [43]. When the attacker has multiple optimal responses to the mixed strategy committed by the defender, a tie occurs. The attacker's various tie-breaking rules result in different Stackelberg equilibria. In real-world scenarios, we typically assume that the attacker will choose the strategy that benefits the defender, thereby leading to an SSE [44,45]. Hence, the optimal mixed strategy for the defender in an SSE is $s_D \in \Delta(S_D)$, which maximizes $\max\{f_D(s_D, RF(s_D)) : s_D \in \Delta(S_D)\}$, where $\Delta(S_D)$ is the set of probability distributions over $S_D$ and $RF(s_D) = \arg\max\{f_A(s_D, s_A) : s_A \in S_A\}$ is the reaction function for the attacker.

## 3. Stackelberg Game Model Based on Interval-Valued Intuitionistic Fuzzy Theory

### *3.1. Basic Assumptions*

Consider a target network, such as a railway network, that is formalized in terms of a simple undirected graph $G(V, E)$, where $V = \{v_1, v_2, \ldots, v_N\}$ 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, respectively, in the railway network). Let $N = |V|$ be the number of nodes in the network. We denote the number of nodes in the network by $N = |V|$. The adjacency matrix $A(G)$ of the network $G$ is defined by $(a_{ij})_{N\times N}$, where $a_{ij} = a_{ji} = 1$ if nodes $v_i$ and $v_j$ are adjacent and $a_{ij} = a_{ji} = 0$ otherwise. The following assumptions are made in this model:

(1) There is only one defender, who moves first, and one attacker, who moves after knowing the defender's strategy commitment.
(2) Both players (i.e., the attacker and the defender) have access to complete information about the target network and possess full knowledge of each other. This means that they are fully informed about all possible strategy profiles and the corresponding payoffs for both sides.
(3) The game consists of a single round, in which both players strive to adopt optimal strategies.

### *3.2. Cost Model*

For node $v_i$, let $c_i^A$ and $c_i^D$ be the attack cost and the defense cost, respectively. The cost $c_i^A$ or $c_i^D$ is determined by a specific referential property $r_i \geq 0$ associated with node $v_i$, which can be expressed as

$$c_i^A = r_i^{q_A}, \tag{5}$$

$$c_i^D = r_i^{q_D}, \tag{6}$$

where $q_A \geq 0$ is the attack cost sensitivity parameter and $q_D \geq 0$ is the defense cost sensitivity parameter. In this paper, the referential property $r_i$ is set as the degree of node $v_i$. From Equations (5) and (6), the cost associated with a node $v_i$ is determined not only by its degree in the network but also by the cost-sensitive parameters of the players. The parameters $q_A$ and $q_D$ can be determined through expert experience, as well as by considering the actual usage and resource allocation of the infrastructure network.

The available resources of both the attacker and the defender can be defined as follows:

$$C^A = \theta_A \sum_{i=1}^{N} c_i^A = \theta_A \sum_{i=1}^{N} r_i^{q_A}, \tag{7}$$

$$C^D = \theta_D \sum_{i=1}^{N} c_i^D = \theta_D \sum_{i=1}^{N} r_i^{q_D}. \tag{8}$$

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 $\theta_A$ and $\theta_D$ represent the attacker's and defender's respective cost budgets for attacking or defending.

### 3.3. Strategies

Based on the cost model presented in Section 3.2, and taking the attacker as an example, the feasible strategies presented in prior studies are defined as follows [13,17].

Suppose that $X = [x_1, x_2, \ldots, x_N] \in S_A$ 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 $\left(v_i \in V^A\right)$; otherwise, $x_i = 0$. The total cost of an attack strategy $X$ is denoted by

$$C_X = \sum_{v_i \in V^A} c_i^A = \sum_{i=1}^{N} x_i c_i^A = \sum_{i=1}^{N} x_i r_i^{q_A}. \tag{9}$$

The cost constraint on the attacker is

$$C_X = \sum_{i=1}^{N} x_i r_i^{q_A} \leq C^A = \theta_A \sum_{i=1}^{N} r_i^{q_A}. \tag{10}$$

Similarly, the cost constraint on the defender is

$$C_Y = \sum_{i=1}^{N} y_i r_i^{q_D} \leq C^D = \theta_D \sum_{i=1}^{N} r_i^{q_D}. \tag{11}$$

In an infrastructure network, when one node fails, its function within the network becomes invalid. We assume that node $v_i$ will only fail if it is attacked without protection (i.e., $x_i = 1$ and $y_i = 0$). Conversely, if the node is defended (i.e., $x_i = 1$ and $y_i = 1$), it will not fail.

The attack and defense strategies defined in Equations (10) and (11) have an expansive strategy space, especially in networks with a large size $N$. For instance, in a network with $N = 100$, $|S_A| = C_N^{N/2} = (100 \times 99 \times \ldots \times 51)/(50 \times 49 \times \ldots \times 1) \geq 2^{50}$ when $\theta_A = 0.5$ and $q_A = 0$. The size of strategy profiles $|S_A| \times |S_D|$ is even larger.

In real-world scenarios, it can be intuitively seen that many decision makers generally choose a better strategy from several options. While there may exist alternative strategies, focusing on the analysis of typical strategies holds greater relevance for decision makers. Therefore, to facilitate the analysis, this paper will consider the following two typical attack and defense strategies [19].

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

To obtain an HS (or LS), the nodes are initially sorted in either descending or ascending order based on their referential property. Subsequently, the targets of the attack (or defense) set are incrementally added in this ordered sequence, while continuously checking for any violation of the cost constraint. This process is terminated when adding one more node into the set results in a violation of the constraint.

### 3.4. Payoffs

To better address uncertainty in attack and defense games in infrastructure networks, it is appropriate to define the payoff for a decision maker as an IVIFN, which is more realistic when dealing with the decision maker's fuzziness. The payoff functions of the attacker and the defender under this circumstance can be represented as $\tilde{f}_A : S_D \times S_A \to IVIFN$ and $\tilde{f}_D : S_D \times S_A \to IVIFN$, respectively. Consider the target network $G(V, E)$, and let $\hat{V} \subseteq V$ be the set of failing nodes and $\hat{E} \subseteq E$ be the set of removed edges. When a node fails, it loses its ability to maintain its functionality, resulting in the removal of all edges connected to it. $\hat{G} = (V, E - \hat{E})$ denotes the network topology that remains after the attack

and defense game is played in a single round. From the perspective of both the attacker and the defender, the change in network topology in the target network $G$ is considered to be the universe of discourse $Z$. The "satisfaction with the effect of the attack or defense" for the attacker and the defender, when the attacker chooses strategy $i$ and the defender takes strategy $j$, is represented by the IVIFN on $Z$, denoted by $\left\langle \left[\mu_{ij}^{AL}, \mu_{ij}^{AU}\right], \left[\nu_{ij}^{AL}, \nu_{ij}^{AU}\right] \right\rangle$ and $\left\langle \left[\mu_{ij}^{DL}, \mu_{ij}^{DU}\right], \left[\nu_{ij}^{DL}, \nu_{ij}^{DU}\right] \right\rangle$, respectively. Because there are only two typical strategies considered in this paper, we have $i, j \in \{1, 2\}$, where strategy 1 represents the HS and strategy 2 represents the LS.

To comprehensively show the effect of the attack and the defense on the target network, we adopt the network efficiency ($\Psi$) and the size of the largest connected component ($\Gamma$) as the functions measuring the network performance. Let $\tilde{G} = (V, E - \tilde{E})$ be the network in which all attacked nodes become failing nodes without any defense. The alterations in the network topology under the strategy profiles (i,j) can be quantified utilizing Equations (12)–(15). Furthermore, these equations serve as references for the IVIFN payoffs of the attacker and the defender.

$$\Psi_{ij}^{A} = \frac{\Psi(G) - \Psi(\hat{G})}{\Psi(G)} \in [0, 1], \tag{12}$$

$$\Gamma_{ij}^{A} = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0, 1], \tag{13}$$

$$\Psi_{ij}^{D} = \frac{\Psi(G) - \Psi(\hat{G})}{\Psi(G)} e^{-\frac{\Psi(\hat{G}) - \Psi(\tilde{G})}{\Psi(G)}} \in [0, 1], \tag{14}$$

$$\Gamma_{ij}^{D} = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} e^{-\frac{\Gamma(\hat{G}) - \Gamma(\tilde{G})}{\Gamma(G)}} \in [0, 1]. \tag{15}$$

Obviously, both $\Psi_{ij}^{A}$ and $\Gamma_{ij}^{A}$ can be used to represent the membership degree with respect to the attacker's satisfaction, while both $\Psi_{ij}^{D}$ and $\Gamma_{ij}^{D}$ can be used to represent the nonmembership degree with respect to the defender's dissatisfaction. The membership and nonmembership degrees may vary within certain ranges, and it is more appropriate to consider them as intervals $\left[\mu_{ij}^{AL}, \mu_{ij}^{AU}\right]$ and $\left[\nu_{ij}^{DL}, \nu_{ij}^{DU}\right]$. In this paper, the membership degree of the attacker and the nonmembership degree of the defender can be obtained based on the aforementioned network metrics, as follows:

$$\mu_{ij}^{AL} = \frac{1}{4} \max\left\{\Psi_{ij}^{A}, \Gamma_{ij}^{A}\right\} + \frac{3}{4} \min\left\{\Psi_{ij}^{A}, \Gamma_{ij}^{A}\right\}, \tag{16}$$

$$\mu_{ij}^{AU} = \frac{3}{4} \max\left\{\Psi_{ij}^{A}, \Gamma_{ij}^{A}\right\} + \frac{1}{4} \min\left\{\Psi_{ij}^{A}, \Gamma_{ij}^{A}\right\}, \tag{17}$$

$$\nu_{ij}^{DL} = \frac{1}{4} \max\left\{\Psi_{ij}^{D}, \Gamma_{ij}^{D}\right\} + \frac{3}{4} \min\left\{\Psi_{ij}^{D}, \Gamma_{ij}^{D}\right\}, \tag{18}$$

$$\nu_{ij}^{DU} = \frac{3}{4} \max\left\{\Psi_{ij}^{D}, \Gamma_{ij}^{D}\right\} + \frac{1}{4} \min\left\{\Psi_{ij}^{D}, \Gamma_{ij}^{D}\right\}, \tag{19}$$

where $\mu_{ij}^{AL}, \mu_{ij}^{AU}, \nu_{ij}^{DL}, \nu_{ij}^{DU} \in [0, 1]$ and $\mu_{ij}^{AL} \leq \mu_{ij}^{AU}, \nu_{ij}^{DL} \leq \nu_{ij}^{DU}$. We divide the original intervals $\left[\min\left\{\Psi_{ij}^{A}, \Gamma_{ij}^{A}\right\}, \max\left\{\Psi_{ij}^{A}, \Gamma_{ij}^{A}\right\}\right]$ and $\left[\min\left\{\Psi_{ij}^{D}, \Gamma_{ij}^{D}\right\}, \max\left\{\Psi_{ij}^{D}, \Gamma_{ij}^{D}\right\}\right]$ into smaller intervals and halve the value range to enhance the accuracy.

Specifically, when more nodes are successfully attacked, the defender's dissatisfaction and the attacker's satisfaction increase. To incorporate the subjective preferences of both the attacker and the defender, we modify the expression to reflect the nonmembership of the attacker and the membership of the defender. This can be obtained as follows:

$$\nu_{ij}^{AL} = \left(1 - \mu_{ij}^{AU}\right) \frac{\left(1 - \mu_{ij}^{AU}\right)}{\left(1 - \mu_{ij}^{AL}\right)} e^{-\frac{|\hat{V}|}{|V|} - \varepsilon}, \tag{20}$$

$$\nu_{ij}^{AU} = \left(1 - \mu_{ij}^{AU}\right) e^{-\frac{|\hat{V}|}{|V|} - \varepsilon}, \tag{21}$$

$$\mu_{ij}^{DL} = \left(1 - \nu_{ij}^{DU}\right) \frac{\left(1 - \nu_{ij}^{DU}\right)}{\left(1 - \nu_{ij}^{DL}\right)} e^{-\frac{|\hat{V}|}{|V|} - \varepsilon}, \tag{22}$$

$$\mu_{ij}^{DU} = \left(1 - \nu_{ij}^{DU}\right) e^{-\frac{|\hat{V}|}{|V|} - \varepsilon}, \tag{23}$$

where $\varepsilon$ is a parameter that represents the hesitancy degree of the attacker and the defender, with a higher value of $\varepsilon$ indicating a greater degree of hesitancy. Let $|\hat{V}|$ denote the number of failing nodes and $|V|$ the total number of nodes. Obviously, we have $\nu_{ij}^{AL}, \nu_{ij}^{AU}, \nu_{ij}^{DL}, \nu_{ij}^{DU} \in [0,1]$ and $\nu_{ij}^{AL} \leq \nu_{ij}^{AU}, \nu_{ij}^{DL} \leq \nu_{ij}^{DU}$. As $|\hat{V}|$ increases, the membership degree of the defender and the nonmembership degree of the attacker decrease. Because $e^{-\frac{|\hat{V}|}{|V|}} \leq 1$, it is obvious that the IVIFNs that we propose satisfy the condition $\mu_{ij}^{AU} + \left(1 - \mu_{ij}^{AU}\right) e^{-\frac{|\hat{V}|}{|V|}} \leq 1$, $\left(1 - \nu_{ij}^{DU}\right)\left(1 - e^{-\frac{|\hat{V}|}{|V|}}\right) + \nu_{ij}^{DU} \leq 1$ (i.e., $\mu_{ij}^{AU} + \nu_{ij}^{AU} \leq 1$, $\mu_{ij}^{DU} + \nu_{ij}^{DU} \leq 1$). Therefore, we can obtain the $2 \times 2$ payoff matrix in Figure 2 based on Equations (16)–(23), where $\tilde{f}_A(i,j) = \left\langle \left[\mu_{ij}^{AL}, \mu_{ij}^{AU}\right], \left[\nu_{ij}^{AL}, \nu_{ij}^{AU}\right] \right\rangle$ and $\tilde{f}_D(i,j) = \left\langle \left[\mu_{ij}^{DL}, \mu_{ij}^{DU}\right], \left[\nu_{ij}^{DL}, \nu_{ij}^{DU}\right] \right\rangle$. The row player is the attacker, and the column player is the defender.

| Attacker \ Defender | HS | LS |
|---|---|---|
| HS | $\tilde{f}_A(1,1), \tilde{f}_D(1,1)$ | $\tilde{f}_A(1,2), \tilde{f}_D(1,2)$ |
| LS | $\tilde{f}_A(2,1), \tilde{f}_D(2,1)$ | $\tilde{f}_A(2,2), \tilde{f}_D(2,2)$ |

**Figure 2.** Payoff matrix of the IVIFS game for the attacker.

The process of generating the IVIFN payoffs of the attacker and the defender under different strategy profiles is shown in Figure 3.

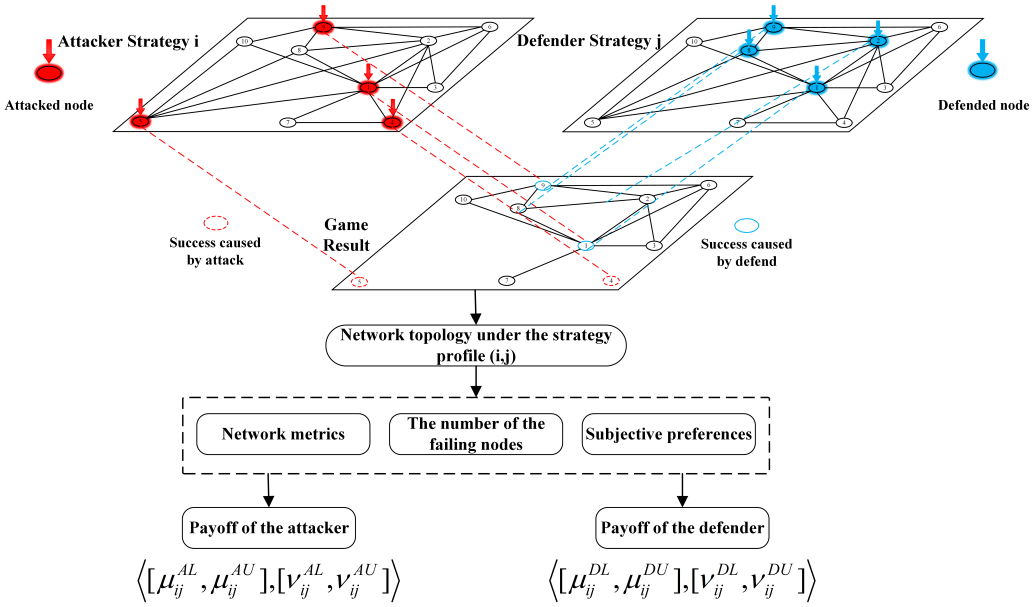



**Figure 3.** The process used to generate the IVIFN payoffs of the attacker and the defender in the proposed game model. A network with 10 nodes is shown as an example, and we focus on one game result where the attacker and defender choose strategies involving red and blue nodes, respectively.

## 4. The Lexicographic Method to Solve a Stackelberg Game with IVIFN Payoffs

### *4.1. The Lexicographic Method*

To solve a Stackelberg game in a crisp condition, Conitzer and Sandholm proposed a multiple linear programming (Multi-LP) algorithm to obtain an SSE solution [42]. Inspired by Multi-LP and the concept of SSE, for a Stackelberg game with the payoffs of IVIFNs, we propose a lexicographic solution method to obtain the optimal strategy profile. For every pure attacker strategy $t \in S_A$, let $p_i^t$ represent the probability that the defender commits to the defense strategy $i \in S_D$ and the vector $\boldsymbol{p}^t = \left(p_1^t, p_2^t, \ldots, p_{|S_D|}^t\right)$ denotes the mixed strategy for the defender. We can derive a mixed strategy for the defender such that (1) pure strategy $t$ is the optimal response for the attacker and (2) the mixed strategy maximizes the defender's utility under this constraint. The mixed strategy can be derived by solving the following fuzzy mathematical programming model:

$$\begin{aligned} &\max \sum_{i\in S_D} p_i^t \tilde{f}_D(i,t) \\ &\text{s.t.} \begin{cases} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,j) \leq_{lex} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,t), \forall j \in S_A \\ \sum_{i\in S_D} p_i^t = 1 \\ p_i^t \geq 0, i \in S_D \end{cases}, \end{aligned} \tag{24}$$

where $\sum_{i\in S_D} p_i^t \tilde{f}_A(i,j) = \langle[1-\prod_{i\in S_D}(1-\mu_{ij}^{AL})^{p_i^t}, 1-\prod_{i\in S_D}(1-\mu_{ij}^{AU})^{p_i^t}], [\prod_{i\in S_D}(\nu_{ij}^{AL})^{p_i^t}, \prod_{i\in S_D}(\nu_{ij}^{AU})^{p_i^t}]\rangle$, $\sum_{i\in S_D} p_i^t \tilde{f}_A(i,t) = \langle[1-\prod_{i\in S_D}(1-\mu_{it}^{AL})^{p_i^t}, 1-\prod_{i\in S_D}(1-\mu_{it}^{AU})^{p_i^t}], [\prod_{i\in S_D}(\nu_{it}^{AL})^{p_i^t}, \prod_{i\in S_D}(\nu_{it}^{AU})^{p_i^t}]\rangle$, and $\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t) = \langle[1-\prod_{i\in S_D}(1-\mu_{it}^{DL})^{p_i^t}, 1-\prod_{i\in S_D}(1-\mu_{it}^{DU})^{p_i^t}], [\prod_{i\in S_D}(\nu_{it}^{DL})^{p_i^t}, \prod_{i\in S_D}(\nu_{it}^{DU})^{p_i^t}]\rangle$ are IVIFNs. The lexicographic order relation is $\leq_{\text{lex}}$. From Wang's ranking method in Definition 4, for IVIFNs $\sum_{i\in S_D} p_i^t \tilde{f}_A(i,j)$ and $\sum_{i\in S_D} p_i^t \tilde{f}_A(i,t)$, we have $\sum_{i\in S_D} p_i^t \tilde{f}_A(i,j) \leq_{lex} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,t)$ if and only if

(1) $WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_A(i,j)\right) < WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_A(i,t)\right)$ or

(2) $WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_A(i,j)\right) = WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_A(i,t)\right)$ and $WAF\left(\sum_{i\in S_D} p_i^t \tilde{f}_A(i,j)\right) \leq WAF\left(\sum_{i\in S_D} p_i^t \tilde{f}_A(i,t)\right)$.

According to Definitions 2 and 4, Equation (24) can be converted into a lexicographic max mathematical programming model as follows:

$$lex\max\left(WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t)\right), WAF\left(\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t)\right)\right)$$
$$\text{s.t.}\begin{cases} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,j) \leq_{lex} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,t), \forall j \in S_A \\ \sum_{i\in S_D} p_i^t = 1 \\ p_i^t \geq 0, i \in S_D \end{cases}, \tag{25}$$

where *lex* max indicates the operation of lexicographic maximization.

We develop a lexicographic approach to solve Equation (25) in the sense of Pareto optimality and divide this approach into two stages.

As the scoring function takes priority over the accuracy function in the objective function, the programming model in the first stage is constructed as

$$\max WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t)\right)$$
$$\text{s.t.}\begin{cases} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,j) \leq_{lex} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,t), \forall j \in S_A \\ \sum_{i\in S_D} p_i^t = 1 \\ p_i^t \geq 0, i \in S_D \end{cases}. \tag{26}$$

The optimal mixed strategy of the defender can be obtained from Equation (26), denoted by $\boldsymbol{p}^{t0} = \left(p_1^{t0}, p_2^{t0}, \ldots, p_{|S_D|}^{t0}\right)$. We then have $WSF^{t^*} = WSF\left(\sum_{i\in S_D} p_i^{t0} \tilde{f}_D(i,t)\right)$ and $WAF^{t0} = WAF\left(\sum_{i\in S_D} p_i^{t0} \tilde{f}_D(i,t)\right)$.

In the second stage, the following programming model is constructed:

$$\max WAF\left(\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t)\right)$$
$$\text{s.t.}\begin{cases} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,j) \leq_{lex} \sum_{i\in S_D} p_i^t \tilde{f}_A(i,t), \forall j \in S_A \\ WSF^{t^*} \leq WSF\left(\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t)\right) \\ WAF^{t0} \leq WAF\left(\sum_{i\in S_D} p_i^t \tilde{f}_D(i,t)\right) \\ \sum_{i\in S_D} p_i^t = 1 \\ p_i^t \geq 0, i \in S_D \end{cases}. \tag{27}$$

By solving Equation (27), we can obtain $WSF^{t*} = WSF\left(\sum_{i\in S_D} p_i^{t*} \tilde{f}_D(i,t)\right)$, $WAF^{t*} = WAF\left(\sum_{i\in S_D} p_i^{t*} \tilde{f}_D(i,t)\right)$ and the optimal strategy $\boldsymbol{p}^{t*} = \left(p_1^{t*}, p_2^{t*}, \ldots, p_{|S_D|}^{t*}\right)$.

For each pure strategy $t$ of the attacker, we can compute the optimal mixed strategy $\boldsymbol{p}^{t*} = \left(p_1^{t*}, p_2^{t*}, \ldots, p_{|S_D|}^{t*}\right)$ and the IVIFN utility $\sum_{i\in S_D} p_i^{t*} \tilde{f}_D(i,t)$ for the defender. Among these attacker strategies, we choose $\hat{t}$ to maximize the defender's IVIFN utility, where $\sum_{i\in S_D} p_i^{\hat{t}*} \tilde{f}_D(i,\hat{t}) \geq_{lex} \sum_{i\in S_D} p_i^{t*} \tilde{f}_D(i,t)$. The mixed strategy $\boldsymbol{p}^{\hat{t}*} = \left(p_1^{\hat{t}*}, p_2^{\hat{t}*}, \ldots, p_{|S_D|}^{\hat{t}*}\right)$ of the defender and strategy $\hat{t}$ of the attacker constitute an optimal strategy profile.

We utilize the aforementioned lexicographic method to solve an example Stackelberg game, where the payoffs are represented by IVIFNs. Let us assume that the risk attitude parameter $\lambda = 0.5$ and the payoff matrices for the attacker and defender are provided as follows:

$$\tilde{A}_e = \begin{array}{c} \\ 1 \\ 2 \end{array}\begin{array}{c} \begin{array}{cc} 1 & 2 \end{array} \\ \begin{pmatrix} \langle[0.2,0.3],[0.2,0.3]\rangle & \langle[0.3,0.4],[0.3,0.4]\rangle \\ \langle[0.5,0.6],[0.1,0.2]\rangle & \langle[0.3,0.8],[0.1,0.2]\rangle \end{pmatrix} \end{array} \tag{28}$$

$$\tilde{D}_e = \begin{array}{c} \\ 1 \\ 2 \end{array}\begin{array}{c} \begin{array}{cc} 1 & 2 \end{array} \\ \begin{pmatrix} \langle[0.5,0.6],[0.2,0.3]\rangle & \langle[0.5,0.6],[0.3,0.4]\rangle \\ \langle[0.4,0.5],[0.1,0.2]\rangle & \langle[0.3,0.4],[0.1,0.2]\rangle \end{pmatrix} \end{array}. \tag{29}$$

The rows of the matrices represent the defender, while the columns represent the attacker. When the attacker chooses strategy 1 and applies Equation (26), a feasible solution $\boldsymbol{p}^{10} = (0,1)$ can be obtained. We then have $WSF^{1*} = 0.6$ and $WAF^{10} = 1.2$. After applying

Equation (27), we find that $\boldsymbol{p}^{1*} = (0,1)$, $WSF^{1*} = 0.6$, and $WAF^{1*} = 1.6$. When the attacker chooses strategy 2 and applies Equation (26), a feasible solution $\boldsymbol{p}^{20} = (0.523, 0.477)$ can be obtained. We then have $WSF^{2*} = 0.463$ and $WAF^{20} = 1.393$. After applying Equation (27), we find that $p^{2*} = (0.523, 0.477)$, $WSF^{2*} = 0.463$, and $WAF^{2*} = 1.393$.

It is evident that the optimal strategy for the defender is (0,1) and that the attacker's best response is strategy 1.

### *4.2. The Lexicographic Algorithm*

The specific calculation process to obtain the equilibria of the Stackelberg game with fuzzy number payoffs is shown in Algorithm 1.

**Algorithm 1** The process to obtain equilibrium strategies

**Input:** The payoff function (or payoff matrix) of the defender, $\tilde{f}_D$;
The payoff function (or payoff matrix) of the attacker, $\tilde{f}_A$;
The strategy set of the defender, $S_D$;
The strategy set of the attacker, $S_A$.

**Output:** The equilibrium payoff of the defender, $\sum_{i \in S_D} p_i^{\hat{t}*} \tilde{f}_D(i, \hat{t})$;
The equilibrium payoff of the attacker, $\sum_{i \in S_D} p_i^{\hat{t}*} \tilde{f}_A(i, \hat{t})$;
The defender's probability distribution when choosing the optimal mixed strategy, $\boldsymbol{p}^{\hat{t}*} = \left(p_1^{\hat{t}*}, p_2^{\hat{t}*}, \ldots, p_{|S_D|}^{\hat{t}*}\right)$;
The attacker's optimal reaction strategy, $\hat{t}$.

**for** $t = 1 : |S_A|$ **do**
  Calculate $WSF^{t*} = \max WSF\left(\sum_{i \in S_D} p_i^t \tilde{f}_D(i,t)\right)$ by Equation (26);
  **if** $WSF^{t*}$ exists **then**
    $\boldsymbol{p}^{t0} = \left(p_1^{t0}, p_2^{t0}, \ldots, p_{|S_D|}^{t0}\right)$;
    $WSF^{t*} = WSF\left(\sum_{i \in S_D} p_i^{t0} \tilde{f}_D(i,t)\right)$;
    Calculate $WAF^{t*} = WAF\left(\sum_{i \in S_D} p_i^t \tilde{f}_D(i,t)\right)$ by Equation (27);
    $\boldsymbol{p}^{t*} = \left(p_1^{t*}, p_2^{t*}, \ldots, p_{|S_D|}^{t*}\right)$;
    $WSF^{t*} = WSF\left(\sum_{i \in S_D} p_i^{t*} \tilde{f}_D(i,t)\right), WAF^{t*} = WAF\left(\sum_{i \in S_D} p_i^{t*} \tilde{f}_D(i,t)\right)$.
  **else if then**
    $WSF^{t*} = -\infty, WAF^{t*} = -\infty$;
  **end if**
**end for**
Sort $\left\{WSF^{t*}\right\}$, $WSF^{\bar{t}*} = \max WSF^{t*}$.
Sort $\left\{WAF^{t*}\right\}$, $WAF^{\hat{t}*} = \max WAF^{\bar{t}*}$.
**return** $\sum_{i \in S_D} p_i^{\hat{t}*} \tilde{f}_D(i, \hat{t})$, $\sum_{i \in S_D} p_i^{\hat{t}*} \tilde{f}_A(i, \hat{t})$, $\boldsymbol{p}^{t*} = \left(p_1^{t*}, p_2^{t*}, \ldots, p_{|S_D|}^{t*}\right)$, $\hat{t}$.

### *4.3. Advantages and Limitations of the Lexicographic Method*

The lexicographic method has the following advantages.

(1) In the lexicographic solution method, the uniqueness of the optimal fuzzy objective values can be guaranteed. It provides a clear and unambiguous ranking of solutions, which is crucial for decision-making processes.
(2) All available information during the solving process, such as the fuzziness of the objectives and the inequality relations within the constraints, is taken into consideration.
(3) The lexicographic method is flexible in the actual decision-making process due to the availability of various similar ranking methods for IVIFNs.

Despite its advantages, the lexicographic method has some limitations.

(1) The proposed method in this paper heavily relies on the input data in the form of IVIFNs. Insufficient or inaccurate payoffs will directly impact the results obtained by the algorithm.

(2) The method proposed in this paper is only applicable to a two-player Stackelberg game and cannot address scenarios with multiple leaders or multiple followers.

## 5. Experiments

### *5.1. Experimental Settings*

We model a scale-free network with a power-law degree distribution, denoted by $p(k) \sim (\eta - 1)m^{\eta-1}k^{-\eta}$ [46], to represent infrastructure networks such as power grids, which often exhibit this type of distribution [47]. We set $N = 300, \eta = 3$, $m = 2$ and the cost-sensitive parameter $q_A = q_D = 0.5$.

To investigate the effect of hesitancy parameter $\varepsilon$, we set $\theta_A = 0.3$ and $\theta_D = 0.7$. According to Definition 1, we present the hesitancy degree for the attacker and defender under different strategy profiles as $\varepsilon$ increases in Table 1. As shown in Table 1, the hesitancy degree under different strategy profiles also increases with the increase in $\varepsilon$. However, considering real-world scenarios, decision makers typically have a certain hesitancy degree, but it is not excessively high. Therefore, choosing $\varepsilon = 0.1$ is a more realistic option. Thus, we set $\varepsilon = 0.1$ in this paper.

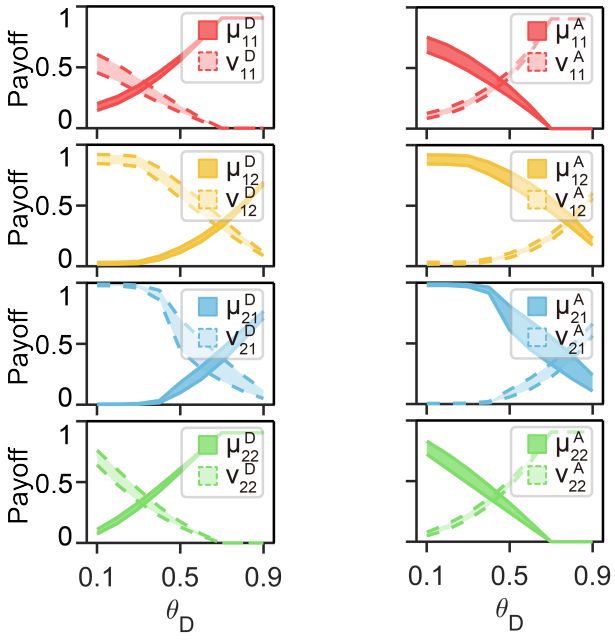
**Table 1.** The hesitancy degree for the attacker and defender under different strategy profiles versus $\varepsilon$.

| $\varepsilon$ | | **0.1** | **0.3** | **0.5** | **0.7** | **0.9** |
|---|---|---|---|---|---|---|
| Attacker's hesitancy | (HS, HS) | [0.10, 0.10] | [0.26, 0.26] | [0.39, 0.39] | [0.50, 0.50] | [0.59, 0.59] |
| | (HS, LS) | [0.17, 0.34] | [0.23, 0.38] | [0.27, 0.42] | [0.30, 0.44] | [0.33, 0.47] |
| | (LS, HS) | [0.11, 0.45] | [0.18, 0.50] | [0.23, 0.53] | [0.28, 0.56] | [0.31, 0.59] |
| | (LS, LS) | [0.10, 0.10] | [0.26, 0.26] | [0.39, 0.39] | [0.50, 0.50] | [0.59, 0.59] |
| Defender's hesitancy | (HS, HS) | [0.10, 0.10] | [0.26, 0.26] | [0.39, 0.39] | [0.50, 0.50] | [0.59, 0.59] |
| | (HS, LS) | [0.18, 0.34] | [0.23, 0.38] | [0.27, 0.42] | [0.31, 0.45] | [0.34, 0.47] |
| | (LS, HS) | [0.12, 0.45] | [0.18, 0.50] | [0.24, 0.53] | [0.28, 0.56] | [0.32, 0.59] |
| | (LS, LS) | [0.10, 0.10] | [0.26, 0.26] | [0.39, 0.39] | [0.50, 0.50] | [0.59, 0.59] |

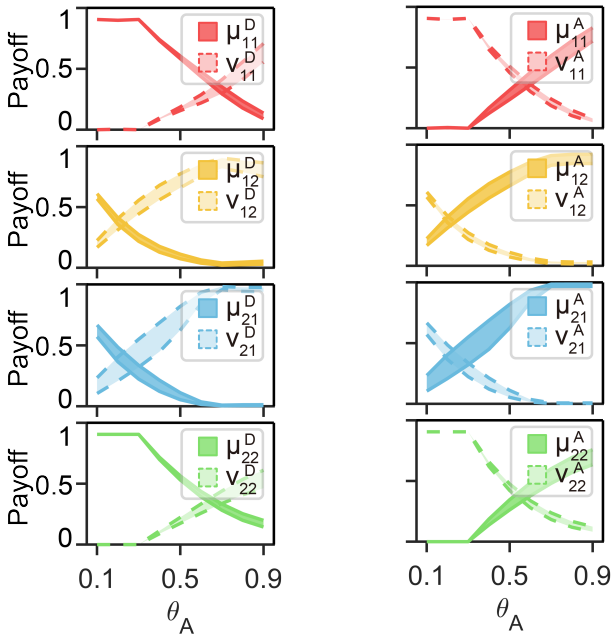
### *5.2. Payoff Analysis*

In Section 3.4, we utilized IVIFNs to represent the payoffs of the attacker and the defender under different strategy profiles in a Stackelberg game in infrastructure networks. This approach was adopted due to the diversity of complex network metrics and the subjective preferences of the players. We analyze the payoffs of the attacker and defender under different strategy profiles when, for example, $\theta_A = 0.7$ and $\theta_D = 0.3$ (Figure 4a,b and Figure 4c,d, respectively), where $\mu_{ij}^A = \left[\mu_{ij}^{AL}, \mu_{ij}^{AU}\right], \nu_{ij}^A = \left[\nu_{ij}^{AL}, \nu_{ij}^{AU}\right]$, $\mu_{ij}^D = \left[\mu_{ij}^{DL}, \mu_{ij}^{DU}\right]$, and $\nu_{ij}^D = \left[\nu_{ij}^{DL}, \nu_{ij}^{DU}\right] (i, j \in \{1, 2\})$.

From Figure 4, it is evident that when $\theta_A$ or $\theta_D$ varies, for $\forall i \in \{1, 2\}, j \in \{1, 2\}$, the monotonicity of $\mu_{ij}^{AL}\left(\mu_{ij}^{DL}\right)$ is consistent with that of $\mu_{ij}^{AU}\left(\mu_{ij}^{DU}\right)$, while it demonstrates an inverse trend compared to the monotonicity of $\nu_{ij}^{AL}\left(\nu_{ij}^{DL}\right)$ and $\nu_{ij}^{AU}\left(\nu_{ij}^{DU}\right)$. Because $\theta_D$ increases and $\theta_A = 0.7$, the defender's membership in different strategy profiles increases while its nonmembership decreases. On the other hand, the attacker's membership in different strategy profiles decreases while its nonmembership increases. When $\theta_A$ increases and $\theta_D = 0.3$, the defender's membership in different strategy profiles decreases while its nonmembership increases. Conversely, the attacker's membership in different strategy profiles increases while its nonmembership decreases. It is obvious that when the cost constraint parameter for the attacker or the defender increases, this generally results in an upward trend in the payoffs for different strategy profiles. This can be inferred from the degree of membership and nonmembership.




(**a**) $\theta_A = 0.7$ (**b**) $\theta_A = 0.7$

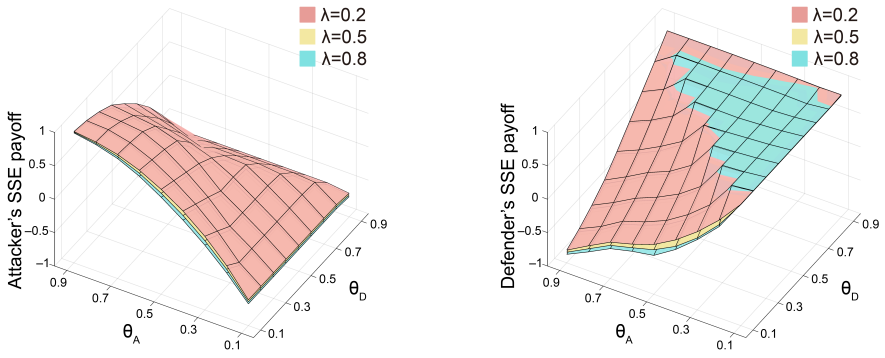



(**c**) $\theta_D = 0.3$ (**d**) $\theta_D = 0.3$

**Figure 4.** The defender's payoffs versus $\theta_D$ (**a**) or $\theta_A$ (**c**) and the attacker's payoffs versus $\theta_D$ (**b**) or $\theta_A$ (**d**) in each strategy profile, where $\theta_A = 0.7$ in (**a**,**b**), $\theta_D = 0.3$ in (**c**,**d**). The payoffs of different strategy profiles are represented as IVIFNs, where the intervals of membership degrees are visually depicted using a darker color and are shown by two solid lines representing the upper and lower bounds. On the other hand, the intervals of nonmembership degrees are depicted with a lighter color and are represented by two dashed lines indicating the upper and lower bounds.

### *5.3. The SSE with Different Values of $\theta_A$ and $\theta_D$*

We use the score function in Definition 4 to show the SSE payoffs of the attacker and the defender (i.e., $WSF\left(\sum_{i\in S_D} p_i^{\hat{t}*} \tilde{f}_A(i,\hat{t})\right)$ and $WSF\left(\sum_{i\in S_D} p_i^{\hat{t}*} \tilde{f}_D(i,\hat{t})\right)$) in Figure 5.




(**a**) Attacker's SSE payoff (**b**) Defender's SSE payoff

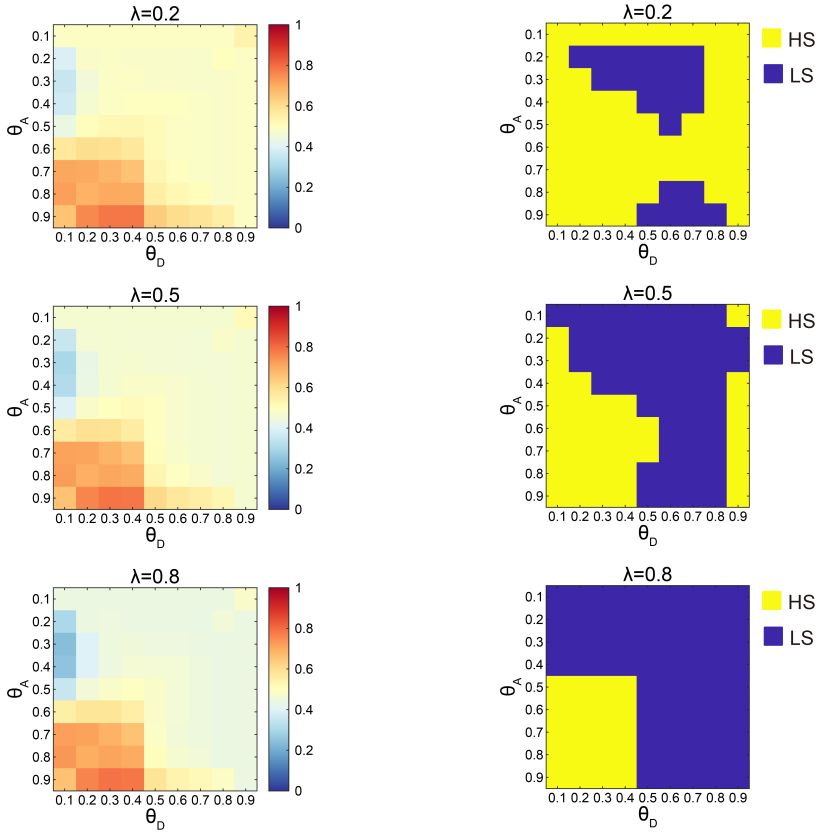
**Figure 5.** SSE payoffs of the attacker (**a**) and the defender (**b**) under different $\lambda$ when $\theta_A, \theta_D \in [0.1, 0.9]$.

In Figure 5a, we can see that the SSE payoffs for the attacker have the highest value when it has significantly more resources than the defender and lowest when the attacker has far fewer resources. Simultaneously, the SSE payoffs of the attacker decrease as $\theta_A$ decreases while $\theta_D$ increases. Conversely, in Figure 5b, we can see that when the defender's resources are much lower than those of the attacker, the defender's SSE payoffs are at their lowest. However, if the defender's resources surpass those of the attacker, the defender's SSE payoffs will be high. Simultaneously, overall, the SSE payoffs for the defender increase as $\theta_A$ decreases while $\theta_D$ increases. However, when $\theta_D$ is greater than $\theta_A$, regardless of the changes in $\theta_D$ or $\theta_A$, the SSE payoffs for the defender remain at their maximum value. This is because when the defender has more resources, the majority of nodes remain unattacked, resulting in higher and relatively unchanged benefits for the defender. Universally, the SSE payoffs of the attacker and the defender will rise with an increase in $\lambda$.

The SSE strategies of the attacker and the defender with different cases of risk attitude parameters are shown in Figure 6. Upon analyzing the SSE strategies of the attacker and the defender, the following two main characteristics can be observed: (1) regarding the defender, regardless of changes in $\lambda$, when $\theta_D$ is small ($\theta_D \in [0.1, 0.4]$) and $\theta_A$ is large ($\theta_A \in [0.6, 0.9]$), the probability of adopting the HS is approximately 0.8; (2) regarding the attacker, regardless of changes in $\lambda$, when $\theta_D$ is small ($\theta_D \in [0.1, 0.4]$) and $\theta_A$ is large ($\theta_A \in [0.6, 0.9]$), the attacker will adopt the HS, and the tendency for the attacker to choose HS increases as $\lambda$ decreases. For these two characteristics, we provide the following explanation.

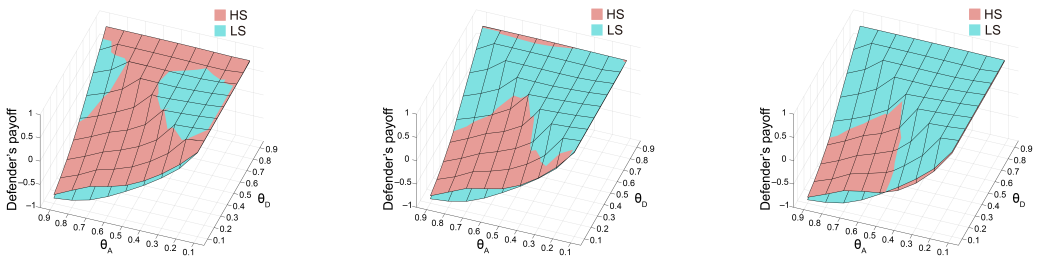
For the first characteristic, when in a weak position, the defender is more likely to allocate its limited resources to protecting critical nodes. This aligns with [6], which states that the failure of critical nodes leads to a significant decline in network performance.

For the second characteristic, Figure 7 shows the defender's optimal utility expressed by the score function in Definition 4 when the best responses of the attacker are the HS and the LS ($WSF\left(\sum_{i\in S_D} p_i^{1*} \tilde{f}_D(i,1)\right)$ and $WSF\left(\sum_{i\in S_D} p_i^{2*} \tilde{f}_D(i,2)\right)$, respectively). According to the theory of breaking ties in SSE, the attacker will choose the best response strategy that maximizes the defender's utility. From Figure 7, when the defender is in a weak position, we always have $WSF\left(\sum_{i\in S_D} p_i^{1*} \tilde{f}_D(i,1)\right) > WSF\left(\sum_{i\in S_D} p_i^{2*} \tilde{f}_D(i,2)\right)$, but as $\lambda$ decreases, situations where $WSF\left(\sum_{i\in S_D} p_i^{1*} \tilde{f}_D(i,1)\right) < WSF\left(\sum_{i\in S_D} p_i^{2*} \tilde{f}_D(i,2)\right)$ become increasingly prevalent. The reason for this is that, by becoming more risk-seeking, the attacker expresses a preference for the HS, which offers an opportunity for greater utility.




(**a**) Defender (**b**) Attacker

**Figure 6.** SSEs of the attacker and the defender when $\theta_A, \theta_D \in [0.1, 0.9]$. The various cases of $\lambda$ are considered. In (**a**), the probabilities of the HS in the defender's mixed SSEs are represented by the colors in the blocks. In (**b**), the HS and the LS are represented by the yellow and blue blocks, respectively.




(**a**) $\lambda = 0.2$ (**b**) $\lambda = 0.5$ (**c**) $\lambda = 0.8$

**Figure 7.** The defender's optimal utility expressed by $WSF$ when the best response of the attacker is HS and LS.

### *5.4. Comparative Analysis*

In order to demonstrate the advantage of taking fuzziness into consideration, we conduct an analysis of the target network using crisp payoffs and the solution method described in [18]. We derive the defender's "crisp strategy" $\boldsymbol{p^c} = \left(p_1^c, p_2^c, \ldots, p_{|S_D|}^c\right)$, where the payoffs are expressed as crisp values obtained solely through the size of the largest connected component, and the solving method employed is the Multi-LP method [42]. By substituting $\boldsymbol{p^c}$ into the proposed model in this paper, we can obtain the attacker's optimal response strategy t by comparing $WSF\left(\sum_{i=S_D} p_i^c \tilde{f}_A(i,j)\right)$, $1 \leq j \leq |S_A|$, which in turn allows us to determine the defender's payoff, represented by the score function

under $\boldsymbol{p}^c$. As an example, we consider the case of $\lambda = 0.5$. We compare the SSE payoffs in Figure 6b with the defender's payoffs under $\boldsymbol{p}^c$, as shown in Figure 8.

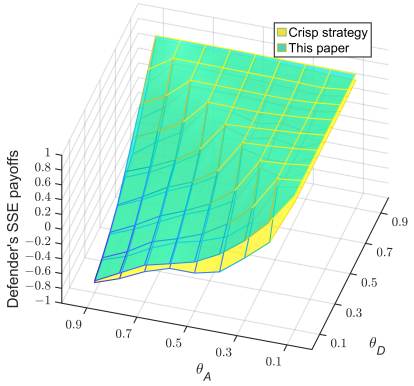



**Figure 8.** Comparison of the SSE payoffs obtained from different models and methods.

From Figure 8, it can be observed that taking the fuzziness into consideration can lead to higher SSE payoffs for the defender. Compared to employing the Multi-LP method under the crisp condition, the defender's SSE payoff can be increased by up to 0.274.

## 6. Conclusions

Critical infrastructure plays a vital role in the stability and development of modern society, and the protection of such infrastructure has recently drawn extensive attention. In this paper, we analyzed the Stackelberg game for an infrastructure network based on IVIF theory, leading to three main contributions.

First, a Stackelberg game model of infrastructure networks with IVIFN payoffs was introduced considering various complex network metrics and the decision makers' subjective judgment. The payoffs of the games in infrastructure networks were evaluated as IVIFNs. To show the effect of an attack on or a defense of the target network in the IVIF environment, the network efficiency and size of the largest connected component were used to represent the membership or nonmembership degree, and we modified the satisfaction of the decision makers according to the number of failed nodes. Second, to solve a Stackelberg game with IVIFN payoffs, we proposed a programming model based on the lexicographic method. In the proposed model, we converted the IVIF constraints into their equivalent sets of crisp constraints and utilized the optimization of a deterministic bi-objective function to be solved in a lexicographic manner. The score function and accuracy function with the risk attitude of the attacker and the defender were used, where the priority of the score function was higher than that of the accuracy function. Combined with the proposed model, we designed an algorithm that would utilize the concept of SSE to determine the optimal strategies for the attacker and the defender. Finally, we investigated the IVIFN payoffs and SSEs of the game in a target scale-free network with different cost constraint parameters for the attacker and the defender. We demonstrated the variation in the trends of the payoffs represented by IVIFNs and discovered that the payoffs of both the attacker and the defender were generally monotonic and had opposite trends when changed. We found that under SSE, the defender's probability of choosing the HS was higher when in a weak position and that the attacker would choose the HS more frequently in various combinations when $\lambda$ became lower. We also observed that taking the fuzziness into consideration can lead to higher SSE payoffs for the defender.

This paper studied a Stackelberg game in infrastructure networks with IVIFN payoffs, and an algorithm based on a lexicographic method was proposed to obtain the optimal strategy. In future work, we will investigate a more appropriate method to denote the IVIFN payoffs. This will allow us to better capture the uncertainty of the decision makers' satisfaction and enhance the accuracy of our analysis. Moreover, for the method of ranking

IVIFNs, we will consider using a more appropriate scoring function or accuracy function to improve the quality of the solution.

**Author Contributions:** Conceptualization, Y.D., J.L. and W.L.; methodology, Y.D. and W.L.; software, Y.D.; validation, Y.D.; formal analysis, Y.D. and J.L.; investigation, J.L. and J.R.; writing—original draft preparation, Y.D. and J.R.; writing—review and editing, J.L., W.L. and Z.L.; visualization, Y.D. and J.R. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Data are contained within the article.

**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.

## References

1. Johnson, C.A.; Flage, R.; Guikema, S.D. Feasibility study of PRA for critical infrastructure risk analysis. *Reliab. Eng. Syst. Saf.* **2021**, *212*, 107643. [CrossRef]
2. Suo, W.; Wang, L.; Li, J. Probabilistic risk assessment for interdependent critical infrastructures: A scenario-driven dynamic stochastic model. *Reliab. Eng. Syst. Saf.* **2021**, *214*, 107730. [CrossRef]
3. Lee, C.; Tien, I. Impacts of varying network parameters on the vulnerability and resilience of interdependent critical infrastructure systems. *Sustain. Resilient Infrastruct.* **2022**, *7*, 984–1007. [CrossRef]
4. Liu, S.; Yin, C.; Chen, D.; Lv, H.; Zhang, Q. Cascading failure in multiple critical infrastructure interdependent networks of syncretic railway system. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 5740–5753. [CrossRef]
5. Herrera, M.; Sasidharan, M.; Cassidy, S.; Parlikad, A.K. Performance assessment of a communication infrastructure with redundant topology: A complex network approach. *Comput. Netw.* **2023**, *228*, 109747. [CrossRef]
6. Albert, R.; Jeong, H.; Barabási, A.L. Error and attack tolerance of complex networks. *Nature* **2000**, *406*, 378–382. [CrossRef]
7. Morone, F.; Makse, H.A. Influence maximization in complex networks through optimal percolation. *Nature* **2015**, *524*, 65–68. [CrossRef]
8. Wang, Z.G.; Deng, Y.; Wang, Z.; Wu, J. Disintegrating spatial networks based on region centrality. *Chaos* **2021**, *31*, 061101. [CrossRef]
9. Fan, N.; Pardalos, P.M. Robust optimization of graph partitioning and critical node detection in analyzing networks. In *Proceedings of the 4th International Conference on Combinatorial Optimization and Applications, Kailua-Kona, HI, USA, 18–20 December 2020*; Wu, W., Daescu, O., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; pp. 170–183. [CrossRef]
10. Addis, B.; Aringhieri, R.; Grosso, A.; Hosteins, P. Hybrid constructive heuristics for the critical node problem. *Ann. Oper. Res.* **2016**, *238*, 637–649. [CrossRef]
11. Bernaschi, M.; Celestini, A.; Cianfriglia, M.; Guarino, S.; Italiano, G.F.; Mastrostefano, E.; Zastrow, L.R. Seeking critical nodes in digraphs. *J. Comput. Sci.* **2023**, *69*, 102012. [CrossRef]
12. 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]
13. Li, Y.P.; Tan, S.Y.; Deng, Y.; Wu, J. Attacker-defender game from a network science perspective. *Chaos* **2018**, *28*, 051102. [CrossRef] [PubMed]
14. Fu, C.; Gao, Y.; Zhong, J.; Sun, Y.; Zhang, P.; Wu, T. Attack-defense game for critical infrastructure considering the cascade effect. *Reliab. Eng. Syst. Saf.* **2021**, *216*, 107958. [CrossRef]
15. Sun, J.; Wang, S.; Zhang, J.; Dong, Q. Attack–defense game in interdependent networks: A functional perspective. *J. Infrastruct. Syst.* **2023**, *29*, 04023020. [CrossRef]
16. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending critical infrastructure. *Interfaces* **2006**, *36*, 530–544. [CrossRef]
17. Li, Y.; Qiao, S.; Deng, Y.; Wu, J. Stackelberg game in critical infrastructures from a network science perspective. *Phys. A* **2019**, *521*, 705–714. [CrossRef]
18. 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* **2019**, *29*, 083129. [CrossRef]
19. Zeng, C.Y.; Ren, B.; Liu, H.; Chen, J. Applying the Bayesian Stackelberg active deception game for securing infrastructure networks. *Entropy* **2019**, *21*, 909. [CrossRef]
20. Fu, C.; Zhang, P.; Zhou, L.; Gao, Y.; Du, N. Camouflage strategy of a stackelberg game based on evolution rules. *Chaos Solitons Fractals* **2021**, *153*, 111603. [CrossRef]
21. Qi, G.; Li, J.; Xu, X.; Chen, G.; Yang, K. An attack-defense game model in infrastructure networks under link hiding. *Chaos* **2022**, *32*, 113109. [CrossRef]
22. Qi, G.; Li, J.; Xu, C.; Chen, G.; Yang, K. Attack-defense game model with multi-type attackers considering information dilemma. *Entropy* **2022**, *25*, 57. [CrossRef] [PubMed]

23. Liu, D.; Zhang, Z. Research on robustness of critical information infrastructure based on attack-defensive game model. *J. Phys. Conf. Ser.* **2021**, *1738*, 012112. [CrossRef]
24. Liu, N.; Liu, S.; Chai, Q.; Zheng, W. A method for analyzing Stackelberg attack-defense game model in 5G by tCPSO. *Expert Syst. Appl.* **2023**, *228*, 120386. [CrossRef]
25. Azevedo, H.; Moreira-Filho, C.A. Topological robustness analysis of protein interaction networks reveals key targets for overcoming chemotherapy resistance in glioma. *Sci. Rep.* **2015**, *5*, 16830. [CrossRef] [PubMed]
26. Tomassini, M. Designing robust scale-free networks under targeted link attack using local information. *Physica A* **2023**, *615*, 128563. [CrossRef]
27. Zadeh, L. Fuzzy sets. *Inf. Control* **1965**, *8*, 338–353. [CrossRef]
28. Atanassov, K.T. Intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1986**, *20*, 87–96. [CrossRef]
29. Atanassov, K.T. More on intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1989**, *33*, 37–45. [CrossRef]
30. Atanassov, K.; Gargov, G. Interval valued intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1989**, *31*, 343–349. [CrossRef]
31. Xu, Z. Methods for aggregating interval-valued intuitionistic fuzzy information and their application to decision making. *J. Control Decis.* **2007**, *22*, 215–219.
32. Wang, F.; Wan, S. Possibility degree and divergence degree based method for interval-valued intuitionistic fuzzy multi-attribute group decision making. *Expert Syst. Appl.* **2020**, *141*, 112929. [CrossRef]
33. Wan, S.; Xu, G.; Dong, J. An Atanassov intuitionistic fuzzy programming method for group decision making with interval-valued Atanassov intuitionistic fuzzy preference relations. *Appl. Soft Comput.* **2020**, *95*, 106556. [CrossRef]
34. Wang, F.; Wan, S. A comprehensive group decision-making method with interval-valued intuitionistic fuzzy preference relations. *Soft Comput.* **2021**, *25*, 343–362. [CrossRef]
35. Wei, A.; Li, D.; Lin, P. An information-based score function of interval-valued intuitionistic fuzzy sets and its application in multiattribute decision making. *Soft Comput.* **2021**, *25*, 1913–1923. [CrossRef]
36. Chen, Z.; Wan, S.; Dong, J. An integrated interval-valued intuitionistic fuzzy technique for resumption risk assessment amid COVID-19 prevention. *Inf. Sci.* **2023**, *619*, 695–721. [CrossRef] [PubMed]
37. Dong, J.; Wan, S. Interval-valued intuitionistic fuzzy best-worst method with additive consistency. *Expert Syst. Appl.* **2024**, *236*, 121213. [CrossRef]
38. Li, D.F. Mathematical-programming approach to matrix games with payoffs represented by Atanassov's interval-valued intuitionistic fuzzy sets. *IEEE Trans. Fuzzy Syst.* **2010**, *18*, 1112–1128. [CrossRef]
39. Xia, M. Interval-valued intuitionistic fuzzy matrix games based on Archimedean t-conorm and t-norm. *Int. J. Gen. Syst.* **2018**, *47*, 278–293. [CrossRef]
40. Kumar, S.; Kumar, M. A game theoretic approach to solve multiple group decision making problems with interval-valued intuitionistic fuzzy decision matrices. *Int. J. Manag. Sci. Eng. Manag.* **2021**, *16*, 34–42. [CrossRef]
41. Naqvi, D.R.; Verma, R.; Aggarwal, A.; Sachdev, G. Solutions of matrix games involving linguistic interval-valued intuitionistic fuzzy sets. *Soft Comput.* **2023**, *27*, 783–808. [CrossRef]
42. Sandholm, V.C. Computing the Optimal Strategy to Commit to. In Proceedings of the EC '06: 7th ACM Conference on Electronic Commerce, Ann Arbor, MI, USA, 11–15 June 2006.
43. Leitmann, G. On generalized Stackelberg strategies. *J. Optim. Theory Appl.* **1978**, *26*, 637–643. [CrossRef]
44. Breton, M.; Alj, A.; Haurie, A. Sequential Stackelberg equilibria in two-person games. *J. Optim. Theory Appl.* **1988**, *59*, 71–97. [CrossRef]
45. Kiekintveld, C.; Jain, M.; Tsai, J.; Pita, J.; Ordóñez, F.; Tambe, M. Computing Optimal Randomized Resource Allocations for Massive Security Games. In Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems, AAMAS '09, Budapest, Hungary, 10–15 May 2009; International Foundation for Autonomous Agents and Multiagent Systems: Richland, SC, USA, 2009; Volume 1, pp. 689–696.
46. Barabási, A.L.; Albert, R. Emergence of scaling in random networks. *Science* **1999**, *286*, 509–512. [CrossRef] [PubMed]
47. Nesti, T.; Sloothaak, F.; Zwart, B. Emergence of scale-free blackout sizes in power grids. *Phys. Rev. Lett.* **2020**, *125*, 058301. [CrossRef]