entropy

MDPI

Article

An Attacker–Defender Game Model with Constrained Strategies

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

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

Abstract: Recently, research interest in the field of infrastructure attack and defense scenarios has increased. Numerous methods have been proposed for studying strategy interactions that combine complex network theory and game theory. However, the unavoidable effect of constrained strategies in complex situations has not been considered in previous studies. This study introduces a novel approach to analyzing these interactions by including the effects of constrained strategies, a factor often neglected in traditional analyses. First, we introduce the rule of constraints on strategies, which depends on the average distance between selected nodes. As the average distance increases, the probability of choosing the corresponding strategy decreases. Second, we establish an attacker–defender game model with constrained strategies based on the above rule and using information theory to evaluate the uncertainty of these strategies. Finally, we present a method for solving this problem and conduct experiments based on a target network. The results highlight the unique characteristics of the Nash equilibrium when setting constraints, as these constraints influence decision makers' Nash equilibria. When considering the constrained strategies, both the attacker and the defender tend to select strategies with lower average distances. The effect of the constraints on their strategies becomes less apparent as the number of attackable or defendable nodes increases. This research advances the field by introducing a novel framework for examining strategic interactions in infrastructure defense and attack scenarios. By incorporating strategy constraints, our work offers a new perspective on the critical area of infrastructure security.

Keywords: infrastructure attack and defense scenarios; complex networks; game theory; constrained strategies; information theory

Citation: Ren, J.; Liu, J.; Dong, Y.; Li, Z.; Li, W. An Attacker–Defender Game Model with Constrained Strategies. *Entropy* **2024**, *26*, 624. https://doi.org/10.3390/e26080624

Academic Editor: Matjaz Perc

Received: 20 June 2024
Revised: 17 July 2024
Accepted: 23 July 2024
Published: 24 July 2024

1. Introduction

Currently, infrastructure networks, such as water supply networks, aviation networks, and transportation networks, play essential roles in human society [1,2]. Excessive dependency on these networks results in human systems having a wide range of vulnerabilities, including to the threats posed by both terrorists and hackers. For example, the September 11 attacks against the World Trade Center in New York and the Pentagon in Virginia resulted in a significant loss of life and had an enormous impact on the economy and politics. Moreover, networks are also prime targets during times of conflict. Therefore, it is vital to consider adversaries' strategies and understand network interdependencies from a global perspective.

Numerous methods, such as probabilistic risk analyses and data analyses, have been proposed to protect infrastructures [3,4]. These methods are unsuitable for modeling the behavior of intelligent adversaries [3–5]. In these cases, game theory provides an appropriate model framework to address this problem, within which the optimal strategies and interactions of players can be assessed [6,7]. For example, Brown et al. [8] formulated a sequential game model to minimize the operating costs for both attack and defense strategies. Pita et al. [9] employed game theory to examine the complexity of airport security. Zhang et al. [10] proposed a game model to address challenges in factory safety management. Feng et al. [11] took this a

step further by integrating game theory and risk assessments to evaluate protective measures for multiple chemical facilities under the looming threat of attacks. They later expanded their study to incorporate multiple attackers [12]. Zhang et al. [13] investigated resource allocation within security games, while Guan et al. [14] delved into an attack–defense game model that incorporated budget constraints. Zhang et al. [15] transformed the game of an infrastructure problem into a multiobjective optimization model and employed evolutionary algorithms to solve it.

However, importantly, the above studies overlook the complex interactions that exist within infrastructure systems. In reality, interconnected infrastructures form a complex network, wherein the failure of a single facility could potentially affect the entire network. A typical network consists of nodes, edges connecting the nodes, and weights assigned to the edges. Initially, mathematicians believed that real systems could be represented by regular structures such as regular lattices and nearest-neighbor grids. By the late 1950s, Erdős et al. [16] introduced random networks, in which the existence of an edge between two nodes is determined by a probability. Networks generated via this method are referred to as random networks. In recent decades, research on small-world networks and scale-free networks has initiated complex network studies. Watts et al. [17] proposed a small-world network model involving the rewiring of the edges between nodes in a regular network. Barabási et al. [18] introduced the scale-free network model, which is characterized by a few nodes with many connections, resulting in a power-law distribution of the node degrees in this type of network. Li et al. [19] proposed a localized world evolutionary network model by using the world trade web. Comellas [20] introduced a small-world network model with a certain regularity in its node connections from the perspective of graph theory to study the topology of communication networks.

Therefore, it is crucial to consider the comprehensive impact of localized infrastructure failures on the entire infrastructure network. To address this issue, protection measures for infrastructure networks should be analyzed by integrating game theory and complex network theory. Fu et al. [21] developed a static network attack and defense game model to examine the impact of cascading failures. Gu et al. [22] analyzed the significance of the Bayesian Stackelberg game model from the perspective of network science. Zeng et al. [23] used the Bayesian Stackelberg game model and proposed a false network construction method. Qi et al. [24,25] proposed a link-hiding rule and analyzed its optimization impact within the context of dynamic attack and defense games in complex networks. Huang et al. [26] used sequential game theory to model attack and defense games in complex networks and proposed a strategy optimization method. Baykal-Guersoy et al. [27] introduced the concept of an attack number, which considers factors such as the number of affected individuals or the occupancy level of critical infrastructure, as a measurement. They developed a game model to examine the security of transportation networks. Li et al. [28–30] proposed an attack–defense model that takes a network perspective to investigate how network structure and cost constraints influence equilibrium outcomes under two typical strategies. Thompson et al. [31,32] analyzed the potential impacts of intelligent attacks and worst-case interruptions on the U.S. air transportation network. Subsequently, they established a defender–attacker–defender optimization model with three levels and proceeded to solve it. These game models can be roughly divided into two categories. One category is that of the simultaneous game models, where the attacker and the defender do not know their opponent's chosen strategies [28,29,33]. The other category, containing the Stackelberg (sequential) game models, is the one in which the attacker can effectively surveil the security measures of the defender [23–25,34–36].

In these studies, it is assumed that players' strategies are not constrained, which is not always possible in realistic situations. In practice, players are often restricted by objective conditions when choosing strategies. Charnes [37] developed the two-person zero-sum constrained game. Owen [38] investigated the existence of solutions to the two-person zero-sum constraint matrix countermeasure problem using dual linear programming theory. Firouzbakht et al. [39] proposed a constrained bimatrix game framework that has practical

applications in various fields, such as modeling packet jamming in wireless networks. Xiao et al. [40] proposed an interval bimatrix game with a constrained strategy.

In this paper, we introduce a new approach to the attacker–defender game model by incorporating strategy constraints. Considering the average distances between nodes is crucial for securing critical infrastructures like high-speed rail (HSR) networks. Shorter distances between stations enable the rapid communication of security signals, essential for swift detection and responses to threats. This quick communication directly impacts the response time of automated security measures. During an attack, shorter distances can significantly reduce the time needed to activate security protocols, mitigating the attack's severity. By incorporating the average node distance as a key metric, our model introduces a method for quantifying the feasibility of strategy selection. The larger the average distance between selected nodes, the more difficult it is to apply that strategy in realistic situations. This approach is not only innovative within the field but also mirrors practical scenarios. We conduct experiments in a target network to analyze the impacts of these constraints.

The rest of the paper is organized as follows: In Section 2, we present some basic assumptions, constrained strategies, and payoffs. In Section 3, the method used for solving the game is presented. The equilibrium results are analyzed in Section 4. Finally, Section 5 concludes the paper.

2. An Attacker–Defender Game Model Based on Constrained Strategies

Considering constrained strategies, we build an attacker–defender game model for infrastructure networks. An infrastructure network can be represented by an undirected simple graph $G(V, E)$, where $V = \{V_1, V_2, \cdots, V_N\}$ represents the node set, $N = |V|$ is the number of nodes, and $E = (e_{ij}) \subseteq V \times V$ represents the link set. Let the adjacency matrix of graph G be $A(G) = (a_{ij})_{N \times N}$. If there is a link between nodes V_i and V_j, then $a_{ij} = a_{ji} = 1$; otherwise, $a_{ij} = a_{ji} = 0$.

Since the actions of the attacker and the defender are simultaneous, this game model is a static model. The attacker–defender game model uses a ten-tuple to represent the confrontation, where $ADG = (N_A, N_D, V^A, S_A, V^D, S_D, P_A, P_D, U_A, U_D)$:

(1) Let N_A represent the attacker in the attacker–defender game model. The attacker predicts the defense strategy of the defender to develop an attack strategy.

(2) Let N_D represent the defender in the attacker–defender game model. The defender predicts the attack strategy of the attacker to develop a defense strategy.

(3) Let V^A represent the attack node set. If the attacker chooses to target nodes V_1 and V_2, then $V^A = \{V_1, V_2\}$.

(4) Let $S_A = \{S_A^1, S_A^2, \cdots, S_A^i, \cdots, S_A^m\}$ represent the attack strategy set. The vector $S_A^i = [x_1, x_2, \cdots, x_N]$ indicates the ith attack strategy in the set of attack strategies. In this case, $x_i = 1$ if the V_i node is attacked ($V_i \subseteq V^A$); otherwise, $x_i = 0$.

(5) Let V^D represent the defense node set. If the defender chooses to target nodes V_3 and V_4, then $V^D = \{V_3, V_4\}$.

(6) Let $S_D = \left\{S_D^1, S_D^2, \cdots, S_D^j, \cdots, S_D^n\right\}$ represent the defense strategy set. The vector $S_D^j = [y_1, y_2, \cdots, y_N]$ indicates the jth defense strategy in the set of defense strategies. In this case, $y_i = 1$ if the V_i node is defended ($V_i \subseteq V^D$); otherwise, $y_i = 0$.

(7) Let $P_A = \{P_A^1, P_A^2, \cdots, P_A^i, \cdots, P_A^m\}$ represent the probability that the attacker adopts an attack strategy. The element P_A^i indicates that the attacker adopts the S_A^i strategy with a probability of P_A^i.

(8) Let $P_D = \left\{P_D^1, P_D^2, \cdots, P_D^j, \cdots, P_D^n\right\}$ represent the probability that the defender adopts a defense strategy. The element P_D^j indicates that the defender adopts the S_D^j strategy with a probability of P_D^j.

(9) Let $U_A = U_A(S_A, S_D)$ represent the profit function for the attacker. The value of the function also depends on S_A and S_D. Different attack strategies and different defense strategies generate different profit values for the attacker.

(10) Let $U_D = U_D(S_A, S_D)$ represent the profit function for the defender. The value of the function depends on S_A and S_D. Different attack strategies and different defense strategies generate different profit values for the defender.

2.1. Basic Assumptions

(1) In this game, there are two rational players, namely, the attacker and the defender. Both players possess complete information about the target network, including knowledge of all possible strategies and the objective metrics associated with the network's structure for each strategy profile in the network.

(2) All attacks and defenses are target nodes. A node is considered to be successfully attacked when it is targeted by the attacker without being protected by the defender. Once a node is successfully attacked, all the edges connected to that node are removed from the network.

(3) In this game, both the attacker and the defender independently formulate their strategies without prior knowledge of each other's decisions. This simultaneous move structure is designed to capture scenarios in which each party operates under conditions of strategic secrecy and independent decision-making. Furthermore, the game is structured as a single-shot interaction, implying that there are no subsequent rounds which could provide opportunities for reassessment or adaptation based on an opponent's previous moves.

2.2. Constraint Strategies

The attack strategy's selection probability is denoted as P_A^i, while the defense strategy's selection probability is represented by P_D^j. The strategy constraints are established as follows:

$$P_A^i \leq \alpha_A^i, \quad \forall S_A^i \in S_A, \tag{1}$$

and

$$P_D^j \leq \alpha_D^j, \quad \forall S_D^j \in S_D, \tag{2}$$

where α_A^i and α_D^j are constraint coefficients for the attacker and the defender, respectively, and belong to the interval $(0, 1)$.

Figure 1 provides a detailed illustration of the method used for calculating the strategy selection probability based on the average distance between selected nodes. In an example network comprising 10 nodes, we presume that both the attacker and the defender opt for three nodes for their respective strategies. The shortest paths between each pair of nodes are then meticulously calculated. The figure shows the process of deriving the average of these shortest paths, which forms the foundation for imposing constraints on strategy selection.

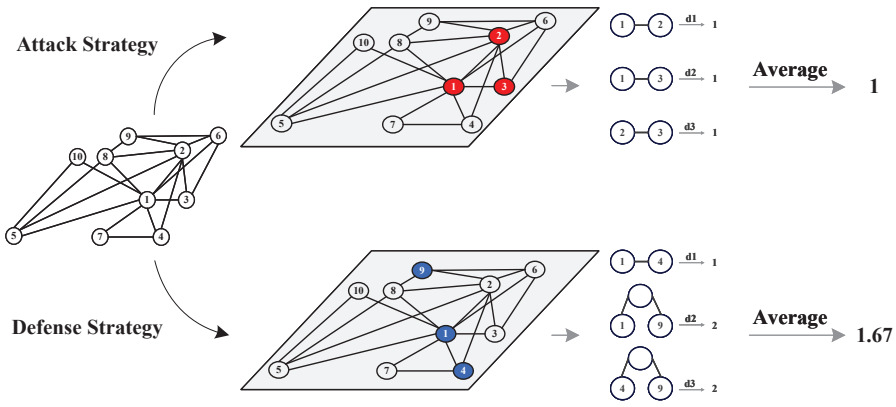

Figure 1. The process of calculating the average distances in this model. The red dots denote the nodes that the attacker chooses to attack and the black dots denote the nodes that the defender chooses to defend.

In this model, as the average distance between selected nodes increases, the probability of choosing their corresponding strategy decreases. We denote the average distance as $\overline{\text{Dist}}_A^i$ for the ith attack strategy and $\overline{\text{Dist}}_D^j$ for the jth defense strategy. We set the strategy constraint rules as follows:

$$C_A^i = \frac{\exp\left(\frac{3}{\overline{\text{Dist}}_A^i}\right)}{\left(\overline{\text{Dist}}_A^i\right)^3}, \quad \forall S_A^i \in S_A, \tag{3}$$

and

$$C_D^j = \frac{\exp\left(\frac{3}{\overline{\text{Dist}}_D^j}\right)}{\left(\overline{\text{Dist}}_D^j\right)^3}, \quad \forall S_D^j \in S_D. \tag{4}$$

Let θ_A represent the attack strategy constraint parameter and θ_D represent the defense strategy constraint parameter. These parameters indicate the strength of the strategy constraints for the two players. The values of θ_A and θ_D depend on the targeted network structures, the players' experience, and their subjective preferences. Larger values of θ_A and θ_D indicate weaker constraints, while smaller values indicate stronger constraints. For the attacker, α_A^i is calculated by

$$\alpha_A^i = \frac{\theta_A\left(C_A^i - \min C_A\right)}{\max C_A - \min C_A}, \quad \forall S_A^i \in S_A, \tag{5}$$

where $\min C_A$ and $\max C_A$ are the minimum and maximum values in $C_A = \{C_A^1, C_A^2, \cdots, C_A^m\}$, respectively.

For the defender, α_D^j is calculated by

$$\alpha_D^j = \frac{\theta_D\left(C_D^j - \min C_D\right)}{\max C_D - \min C_D}, \quad \forall S_D^j \in S_D, \tag{6}$$

where $\min C_D$ and $\max C_D$ are the minimum and maximum values in $C_D = \{C_D^1, C_D^2, \cdots, C_D^n\}$, respectively.

Additionally, we propose incorporating an entropy-based measure to quantify the uncertainty and variability of the strategy selection probabilities. The entropy H of the attack and defense strategies can be defined as follows:

$$H_A = -\sum_i P_A^i \log P_A^i, \tag{7}$$

and

$$H_D = -\sum_j P_D^j \log P_D^j. \tag{8}$$

These entropy measures provide additional insights into the diversity and unpredictability of these strategies. They serve as a metric for assessing the diversity and unpredictability of these strategies.

2.3. Payoffs

In Section 2.1, we assume that node V_i is successfully removed only if it is attacked by the attacker and is not protected by the defender. We define the sets of removed nodes and edges as $\widehat{V} \subseteq V$ and $\widehat{E} \subseteq E$, respectively. Then, the resulting network after its removal can be denoted as $\widehat{G} = (V - \widehat{V}, E - \widehat{E})$.

Here, it is evident that $\widehat{V} = V^A - V^A \cap V^D$. The set of removed nodes $\widehat{V}$ is equal to the set of nodes attacked by the attacker V^A minus the set of nodes attacked by the attacker and protected by the defender $V^A \cap V^D$. This can be shown by the following calculation:

$$\begin{aligned} \widehat{V} &= \{V_i \in V \mid V_i \in V^A \text{ and } V_i \notin V^D\} \\ &= \{V_i \in V^A \mid V_i \notin V^D\} \\ &= V^A - V^D \\ &= V^A - (V^A \cap V^D). \end{aligned} \tag{9}$$

We denote the measure of network performance as Γ, which can be evaluated by the size of the largest connected component [41], efficiency [42], and other metrics. Additionally, we define the attacker's payoff as

$$U_A^{ij}\left(S_A^i, S_D^j\right) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0,1], \tag{10}$$

while the defender's payoff is defined as

$$U_D^{ij}\left(S_A^i, S_D^j\right) = \frac{\Gamma(\hat{G}) - \Gamma(G)}{\Gamma(G)} \in [-1,0], \tag{11}$$

where Γ is defined as the measure of network performance. In this paper, $\Gamma(G)$ and $\Gamma(\hat{G})$ are the sizes of the largest connected component of network $G(V,E)$ and network $\widehat{G} = (V - \widehat{V}, E - \widehat{E})$, respectively. The sum of the attacker's payoff and the defender's payoff is zero, indicating a zero-sum game.

3. Solution

In a constrained game, the attacker's objective is to maximize their payoff under strategy constraints, while the defender aims to minimize their loss. Therefore, we establish a linear programming model with two objectives to solve this problem. Let us suppose that z, ω are the expected payoffs for the attacker and the defender, respectively; then, the model is defined as follows:

$$\begin{aligned} \max \quad & z \\ \text{s.t.} \quad & \textstyle\sum_{S_A^i \in S_A} U_A(S_A^i, S_D^j) \cdot P_A^i \geq z, \forall S_D^j \in S_D \\ & P_A^i \leq \alpha_A^i, \forall S_A^i \in S_A \\ & \textstyle\sum_{S_A^i \in S_A} P_A^i = 1 \\ & P_A^i \geq 0, \forall S_A^i \in S_A, \end{aligned} \tag{12}$$

$$\begin{aligned} \max \quad & \omega \\ \text{s.t.} \quad & \textstyle\sum_{S_D^j \in S_D} U_D(S_A^i, S_D^j) \cdot P_D^j \geq \omega, \forall S_A^i \in S_A \\ & P_D^j \leq \alpha_D^j, \forall S_D^j \in S_D \\ & \textstyle\sum_{S_D^j \in S^D} P_D^j = 1 \\ & P_D^j \geq 0, \forall S_D^j \in S_D, \end{aligned} \tag{13}$$

where $U_A(S_A^i, S_D^j)$ is the payoff for the attacker under strategy profile $\left(S_A^i, S_D^j\right)$ and $U_D(S_A^i, S_D^j)$ is the payoff for the defender. Equation (12) is the optimization model for the attacker, and Equation (13) is the optimization model for the defender. By solving this model, the Nash equilibrium $\left(P_A^*, P_D^*\right)$ is obtained. Then, the equilibrium payoff values for the attacker and the defender are defined as

$$z(P_A^*, P_D^*) = P_A^T U_A P_D = \left(P_A^1, P_A^2, \cdots, P_A^{|S_A|}\right) \begin{pmatrix} u_A^{11} & u_A^{12} & \cdots & u_A^{1|S_D|} \\ u_A^{21} & u_A^{22} & \cdots & u_A^{2|S_D|} \\ \vdots & \vdots & & \vdots \\ u_A^{|S_A|1} & u_A^{|S_A|2} & \cdots & u_A^{|S_A||S_D|} \end{pmatrix} \begin{pmatrix} P_D^1 \\ P_D^2 \\ \vdots \\ P_D^{|S_D|} \end{pmatrix}, \tag{14}$$

and

$$\omega(P_A^*, P_D^*) = P_A^T U_D P_D = \left(P_A^1, P_A^2, \cdots, P_A^{|S_A|}\right) \begin{pmatrix} u_D^{11} & u_D^{12} & \cdots & u_D^{1|S_D|} \\ u_D^{21} & u_D^{22} & \cdots & u_D^{2|S_D|} \\ \vdots & \vdots & & \vdots \\ u_D^{|S_A|1} & u_D^{|S_A|2} & \cdots & u_D^{|S_A||S_D|} \end{pmatrix} \begin{pmatrix} P_D^1 \\ P_D^2 \\ \vdots \\ P_D^{|S_D|} \end{pmatrix}. \tag{15}$$

Due to Equations (10) and (11), we know that this is a zero-sum game, so the payoff for the attacker is equal to the loss of the defender, which is denoted as $z = -\omega$.

4. Experiment

In this section, we conducted experiments to demonstrate the effectiveness of our model, using a high-speed rail (HSR) network as an example. In the context of a high-speed rail network, which spans vast geographical areas with numerous stations and control centers, the average distance between nodes plays a pivotal role in the security strategy used. Consider the security strategy for a major HSR network like China's extensive HSR system, which connects numerous cities across the country. This strategy must ensure the safety and integrity of both passengers and infrastructure. The average distance between stations and control centers is crucial to determine the efficiency and effectiveness of security measures, from real-time monitoring to emergency response coordination.

For comparison purposes, we divided the experiments into two groups: one under unconstrained conditions and the other under constrained conditions. For each group of experiments, we set the number of attackable or defendable nodes to 2, 3, and 4, respectively. We then applied Equations (12) and (13) to generate Nash equilibrium solutions before proceeding with the analysis.

Our analysis was conducted on a system equipped with a 12th Gen Intel Core i7-12700H processor, 32.0 GB of RAM, and a 64-bit operating system running on an x64-based processor. The equipment is from Lenovo, a manufacturer located in Beijing, China. The data originated from the targeted network.

4.1. Experiment without Constrained Strategies

4.1.1. Experimental Setting

In our experiments conducted within a target network, Figure 2 offers a comprehensive visualization of the nodes' significance under various centrality metrics: degree centrality (DC), closeness centrality (CC), betweenness centrality (BC), and eigenvector centrality (EC). This visualization employs a color gradient, with the nodes appearing more red having a higher value for the corresponding centrality metric.

Degree centrality (DC) [43]: This is a measure that quantifies the direct influence of a node on a network. It is based on the principle that nodes with higher degrees have a greater potential to directly affect their neighbors, thereby increasing their significance

within the network. The degree of i is $k_i = \sum_{j=1}^{n} a_{ij}$, which is equal to the number of edges connected to it. This is calculated by

$$\mathrm{DC}(i) = \frac{k_i}{N-1}, \tag{16}$$

where N denotes the total number of nodes in G and $N-1$ is the maximum possible degree. For normalization, the equation is divided by N-1 based on the degree.

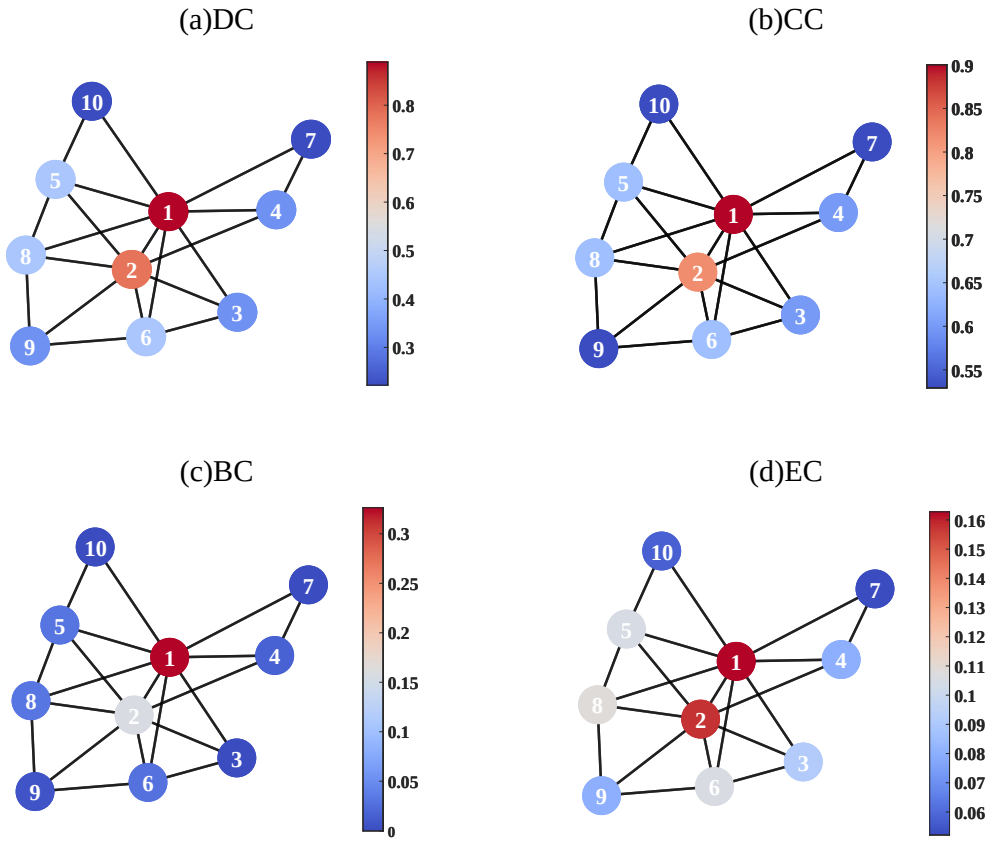

Figure 2. This figure shows the importance of the nodes in terms of various metrics, including degree centrality (DC), closeness centrality (CC), betweenness centrality (BC), and eigenvector centrality (EC). The nodes' influence is represented by the color of the nodes.

Closeness centrality (CC) [44]: This metric is based on the average time it takes for information to travel from one node to another. It quantifies how quickly a node can reach all other nodes in the network. The closeness centrality of a node is calculated as the sum of the reciprocals of the shortest distances from that node to all other nodes divided by the number of nodes in the network. This value represents the average transmission time needed for information to travel from one node to all other nodes in the network. Nodes with higher closeness centrality values are considered more important because they have greater access to information and can influence the network more quickly. CC is calculated by

$$\mathrm{CC}(i) = \frac{1}{N-1} \sum_{j \neq i} \frac{1}{d_{ij}}, \tag{17}$$

where d_{ij} represents the average shortest distance from node V_i to node V_j. If there is no connection between V_i and V_j, the distance approaches infinity, in which case $\frac{1}{d_{ij}} = \frac{1}{\infty} = 0$.

Betweenness centrality (BC) [45]: This is a measure of the influence of a node on the flow of information in a network. This measure quantifies how many shortest paths pass through a particular node and, in turn, how many other nodes are reachable from

those paths. The betweenness centrality of a node is calculated by summing the number of shortest paths that pass through each of its neighbors, weighted by the number of shortest paths that include those neighbors. Nodes with higher betweenness centrality values are considered more influential as they play a crucial role in connecting different parts of the network and distributing information efficiently. BC is calculated by

$$\mathrm{BC}(i) = \frac{2}{N(N-1)} \sum_{s \neq t \neq i} \frac{g_{st}(i)}{g_{st}}, \tag{18}$$

where $g_{st}(i)$ represents the number of shortest paths from node s to node t through node i. g_{st} represents the total number of shortest paths from node s to node t.

Eigenvector centrality (EC) [46]: This metric is a measure of the importance of nodes in a network based on the quality of their connections to other nodes. EC quantifies how influential a node is by accounting for not only the number of its neighbors but also the importance of those neighbors. This is calculated by

$$\mathrm{EC}(i) = \frac{1}{\lambda} \sum_{j=1}^{n} a_{ij} f_j, \tag{19}$$

where a_{ij} is the adjacency matrix of the network, f_j is the value of the jth entry of the normalized largest eigenvector, and λ is a constant.

This network consists of 10 nodes and 20 edges. Among the nodes, V_1 and V_2 have high values and V_7 and V_{10} have low values. In this model, a objective function is established based on the size of the largest connected component. We conducted this experiment with different numbers of nodes to be attacked or defended.

4.1.2. The Nash Equilibrium

The mixed-strategy Nash equilibrium results are presented in Tables 1–3. Notably, the pure strategies with nonzero probabilities in their equilibrium are listed, as are their respective probabilities. From the equilibrium results when $|V^A| = |V^D| = 2$, we observe that the attacker has five pure strategies with nonzero probabilities. On the one hand, the highest probabilities are assigned to the attack strategies $\{V_3, V_8\}$, $\{V_4, V_{10}\}$, $\{V_5, V_7\}$, and $\{V_6, V_9\}$, all of which have a probability of 0.23077. On the other hand, strategy $\{V_1, V_2\}$ has the lowest probability. Notably, V_1 and V_2 have high values for the centrality properties examined in this network. For the defender, strategies $\{V_1, V_6\}$, $\{V_1, V_7\}$, $\{V_1, V_9\}$, and $\{V_2, V_8\}$ have the highest probabilities, all equal to 0.15385, with V_1 having the highest value for the centrality properties. When $|V^A| = |V^D| = 3$, the nonzero probabilities of each strategy chosen by both the attacker and defender are given in Table 2. For example, strategy $\{V_2, V_6, V_8\}$ has the highest probability among the attacker's strategies, with a value of 0.2093, and the probability of the defender selecting strategy $\{V_1, V_6, V_9\}$ is 0.25. Similarly, in the third scenario, where $|V^A| = |V^D| = 4$, there are a total of eight attack strategies and seven defense strategies with nonzero probabilities. Table 3 provides the probabilities for each strategy. The attacker is more likely to choose strategy $\{V_3, V_4, V_6, V_{10}\}$, while the defender tends to choose strategies $\{V_1, V_6, V_7, V_9\}$ and $\{V_2, V_4, V_5, V_{10}\}$.

It is evident that some strategies are much more likely to be chosen than others. For example, in the three scenarios, certain attack and defense strategies have probabilities close to 0.2 or 0.3, respectively. Additionally, by comparing the three scenarios using different values of $|V^A|$ and $|V^D|$, we can see that the number of nodes to be attacked or defended affects the players' decision-making results. With an increased number of nodes, players have more flexibility in choosing their strategies, leading to a more complex game.

Table 1. The mixed-strategy Nash equilibrium results without constraints ($|V^A| = |V^D| = 2$).

Attack strategy	$\{V_3, V_8\}$	$\{V_4, V_{10}\}$	$\{V_5, V_7\}$	$\{V_6, V_9\}$	$\{V_1, V_2\}$
Probability	0.23077	0.23077	0.23077	0.23077	0.076923
Defense strategy	$\{V_1, V_6\}$	$\{V_1, V_7\}$	$\{V_1, V_9\}$	$\{V_2, V_8\}$	$\{V_4, V_{10}\}$
Probability	0.15385	0.15385	0.15385	0.15385	0.15385
Defense strategy	$\{V_1, V_5\}$	$\{V_2, V_3\}$	$\{V_3, V_5\}$		
Probability	0.076923	0.076923	0.076923		

Table 2. The mixed-strategy Nash equilibrium results without constraints ($|V^A| = |V^D| = 3$).

Attack strategy	$\{V_2, V_6, V_8\}$	$\{V_3, V_7, V_{10}\}$	$\{V_7, V_9, V_{10}\}$	$\{V_1, V_4, V_5\}$	$\{V_3, V_4, V_9\}$
Probability	0.2093	0.18605	0.13953	0.13953	0.093023
Attack strategy	$\{V_3, V_7, V_9\}$	$\{V_5, V_9, V_{10}\}$	$\{V_3, V_4, V_5\}$		
Probability	0.093023	0.093023	0.046512		
Defense strategy	$\{V_1, V_6, V_9\}$	$\{V_1, V_8, V_{10}\}$	$\{V_2, V_4, V_7\}$	$\{V_2, V_3, V_5\}$	$\{V_3, V_4, V_5\}$
Probability	0.25	0.23837	0.14535	0.14535	0.11047
Defense strategy	$\{V_1, V_2, V_7\}$	$\{V_2, V_7, V_{10}\}$	$\{V_1, V_7, V_8\}$	$\{V_1, V_6, V_7\}$	$\{V_1, V_7, V_9\}$
Probability	0.063953	0.017442	0.017442	0.005814	0.005814

Table 3. The mixed-strategy Nash equilibrium results without constraints ($|V^A| = |V^D| = 4$).

Attack strategy	$\{V_3, V_4, V_6, V_{10}\}$	$\{V_3, V_4, V_9, V_{10}\}$	$\{V_6, V_7, V_8, V_9\}$	$\{V_5, V_7, V_9, V_{10}\}$
Probability	0.19608	0.13725	0.13725	0.13725
Attack strategy	$\{V_1, V_2, V_5, V_8\}$	$\{V_3, V_6, V_7, V_8\}$	$\{V_2, V_4, V_5, V_8\}$	$\{V_3, V_4, V_7, V_8\}$
Probability	0.11765	0.098039	0.078431	0.039216
Attack strategy	$\{V_2, V_6, V_7, V_9\}$	$\{V_4, V_5, V_7, V_9\}$		
Probability	0.039216	0.019608		
Defense strategy	$\{V_1, V_6, V_7, V_9\}$	$\{V_2, V_4, V_5, V_{10}\}$	$\{V_1, V_3, V_8, V_{10}\}$	$\{V_2, V_3, V_5, V_8\}$
Probability	0.32353	0.26471	0.11765	0.058824
Defense strategy	$\{V_1, V_3, V_7, V_8\}$	$\{V_3, V_6, V_8, V_9\}$	$\{V_1, V_3, V_4, V_8\}$	$\{V_2, V_3, V_4, V_5\}$
Probability	0.058824	0.058824	0.058824	0.029412
Defense strategy	$\{V_2, V_4, V_5, V_8\}$			
Probability	0.029412			

To explore the nodes that the attacker and the defender are most likely to select in the Nash equilibrium, we map the probabilities over pure strategies to those over each node via the following equations:

$$\rho_A = \frac{1}{|V^A|} \sum_{i=1}^{|S_A|} P_A^i \cdot S_A^i, \tag{20}$$

and

$$\rho_D = \frac{1}{|V^D|} \sum_{j=1}^{|S_D|} P_D^j \cdot S_D^j, \tag{21}$$

where $\rho_A = [\tilde{p}_1, \tilde{p}_2, \cdots, \tilde{p}_i, \cdots, \tilde{p}_N]$ and $\rho_D = [\tilde{q}_1, \tilde{q}_2, \cdots, \tilde{q}_j, \cdots, \tilde{q}_N]$ are the probability distributions over each node for two players. With this approach, the selection probability distributions for each node are obtained and mapped from the probabilities in Tables 1–3, as shown in Figure 3.

The nodes with the lowest probabilities of being attacked are V_1 and V_2, whose degree centrality, closeness centrality, betweenness centrality, and eigenvector centrality are the highest. However, the defender allocates the greatest probability to protecting nodes V_1 and V_2. This finding suggests that nodes with greater scores are generally more likely to be

protected. As the number of nodes to be attacked or defended increases, the probability distribution of the nodes becomes more uniform.

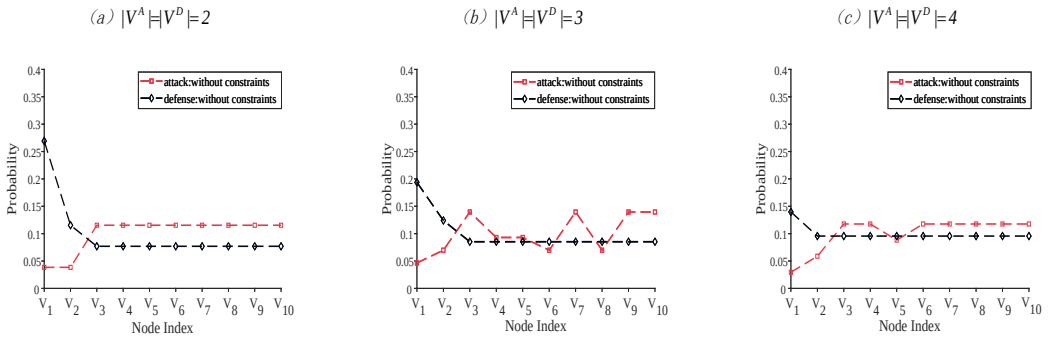

Figure 3. The attack and defense probability distributions for nodes when different numbers of nodes are attacked or defended.

4.2. Experiments with Constrained Strategies

The Nash Equilibrium

As shown in Section 2.2, θ_A and θ_D in Equations (5) and (6) are determined by various factors. In this experiment, we set $\theta_A = 0.25$ and $\theta_D = 0.05$ based on the network structure shown in Figure 2 and the unconstrained Nash equilibrium results in Tables 1–3. However, when $|V^A| = |V^D| = 2$, there is no solution for which $\theta_D = 0.05$. Therefore, when $|V^A| = |V^D| = 2$, we set the critical value $\theta_D = 0.06$.

Tables 4–6 present the mixed-strategy Nash equilibrium results with strategy constraints for scenarios where the numbers of attack and defense nodes are equal ($|V^A| = |V^D| = 2, 3, 4$). These tables show the first ten highest probabilities of each attack and defense strategy being chosen by both players.

Table 4. The mixed-strategy Nash equilibrium results with strategy constraints ($|V^A| = |V^D| = 2$).

Attack strategy	$\{V_1, V_2\}$	$\{V_1, V_5\}$	$\{V_1, V_4\}$	$\{V_4, V_7\}$	$\{V_6, V_7\}$
Probability	0.25	0.20602	0.19518	0.12259	0.027353
Attack strategy	$\{V_4, V_{10}\}$	$\{V_3, V_9\}$	$\{V_3, V_7\}$	$\{V_3, V_{10}\}$	$\{V_4, V_9\}$
Probability	0.026268	0.025993	0.025858	0.025724	0.025525
Defense strategy	$\{V_1, V_2\}$	$\{V_1, V_5\}$	$\{V_1, V_6\}$	$\{V_1, V_8\}$	$\{V_1, V_4\}$
Probability	0.06	0.049444	0.048545	0.048326	0.046842
Defense strategy	$\{V_1, V_3\}$	$\{V_2, V_6\}$	$\{V_2, V_8\}$	$\{V_2, V_5\}$	$\{V_1, V_7\}$
Probability	0.045837	0.045641	0.045254	0.044132	0.04255

Table 5. The mixed-strategy Nash equilibrium results with strategy constraints ($|V^A| = |V^D| = 3$).

Attack strategy	$\{V_6, V_8, V_9\}$	$\{V_1, V_3, V_4\}$	$\{V_1, V_4, V_5\}$	$\{V_1, V_4, V_{10}\}$	$\{V_2, V_4, V_7\}$
Probability	0.048188	0.048188	0.048188	0.048188	0.048188
Attack strategy	$\{V_2, V_6, V_8\}$	$\{V_5, V_8, V_9\}$	$\{V_5, V_8, V_{10}\}$	$\{V_3, V_6, V_9\}$	$\{V_2, V_3, V_9\}$
Probability	0.048188	0.048188	0.048188	0.048188	0.040862
Defense strategy	$\{V_1, V_2, V_4\}$	$\{V_1, V_2, V_3\}$	$\{V_1, V_2, V_5\}$	$\{V_1, V_2, V_6\}$	$\{V_1, V_3, V_6\}$
Probability	0.05	0.05	0.05	0.05	0.05
Defense strategy	$\{V_2, V_5, V_8\}$	$\{V_1, V_2, V_8\}$	$\{V_1, V_4, V_7\}$	$\{V_1, V_5, V_8\}$	$\{V_1, V_5, V_{10}\}$
Probability	0.05	0.05	0.05	0.05	0.05

Table 6. The mixed-strategy Nash equilibrium results with strategy constraints ($|V^A| = |V^D| = 4$).

Attack strategy	$\{V_1, V_2, V_5, V_9\}$	$\{V_3, V_6, V_8, V_9\}$	$\{V_1, V_3, V_4, V_{10}\}$	$\{V_1, V_3, V_7, V_{10}\}$
Probability	0.035504	0.024047	0.024047	0.024047
Attack strategy	$\{V_5, V_6, V_8, V_9\}$	$\{V_1, V_4, V_6, V_{10}\}$	$\{V_1, V_4, V_8, V_{10}\}$	$\{V_2, V_3, V_6, V_7\}$
Probability	0.024047	0.024047	0.024047	0.024047
Attack strategy	$\{V_1, V_3, V_4, V_5\}$	$\{V_2, V_6, V_8, V_9\}$		
Probability	0.024047	0.014469		
Defense strategy	$\{V_1, V_2, V_3, V_6\}$	$\{V_1, V_2, V_3, V_4\}$	$\{V_1, V_2, V_4, V_7\}$	$\{V_1, V_2, V_4, V_8\}$
Probability	0.05	0.020088	0.020088	0.020088
Defense strategy	$\{V_1, V_2, V_6, V_9\}$	$\{V_1, V_2, V_8, V_9\}$	$\{V_1, V_5, V_8, V_{10}\}$	$\{V_1, V_2, V_4, V_5\}$
Probability	0.020088	0.020088	0.020088	0.020088
Defense strategy	$\{V_1, V_2, V_5, V_{10}\}$	$\{V_2, V_5, V_8, V_9\}$		
Probability	0.020088	0.020088		

When $|V^A| = |V^D| = 2$, compared to the result without any constraints, it is obvious that both the attacker and the defender are more likely to choose strategies $\{V_1, V_2\}$ and $\{V_1, V_5\}$. For the attacker, the probability of selecting strategy $\{V_1, V_2\}$ is 0.25, and the probability of choosing $\{V_1, V_5\}$ is 0.20602. For the defender, the probabilities of selecting $\{V_1, V_2\}$ or $\{V_1, V_5\}$ are 0.06 or 0.049444, respectively.

When $|V^A| = |V^D| = 3, 4$, the probability distribution becomes more uniform. Certain strategies share equal probabilities. For instance, when $|V^A| = |V^D| = 3$, the probabilities of the attacker choosing attack strategies $\{V_6, V_8, V_9\}$, $\{V_1, V_3, V_4\}$, $\{V_1, V_4, V_5\}$, and so on, are all 0.048188. Similarly, the probabilities of the defender selecting defense strategies $\{V_1, V_2, V_4\}$, $\{V_1, V_2, V_3\}$, $\{V_1, V_2, V_5\}$, and so on, are all 0.05. When $|V^A| = |V^D| = 4$, the probability of the attacker choosing attack strategy $\{V_1, V_2, V_5, V_9\}$ is 0.035504, and the probability of them choosing strategies $\{V_3, V_6, V_8, V_9\}$, $\{V_1, V_3, V_4, V_{10}\}$, and so on, is 0.024047. Similarly, the probability of the defender selecting defense strategies $\{V_1, V_2, V_3, V_6\}$, $\{V_1, V_2, V_3, V_4\}$, $\{V_1, V_2, V_4, V_7\}$, and so on, is 0.020088.

4.3. The Probability Distribution of Each Node

Subsequently, we obtain the distribution of probability across nodes based on Equations (20) and (21). To analyze the various constraints effectively, we have illustrated them in Figure 4.

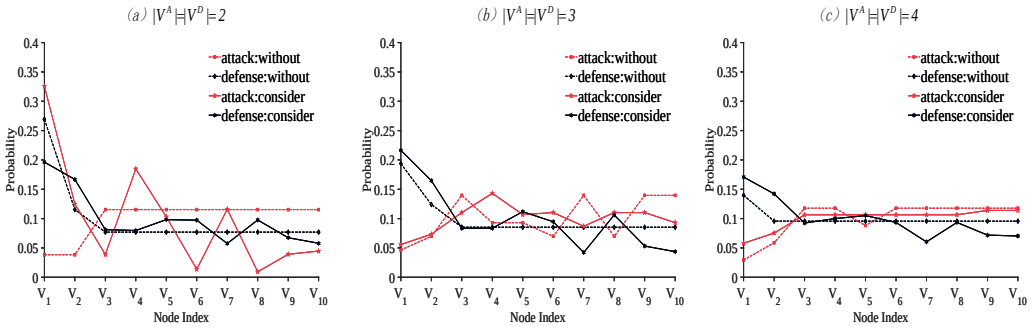

Figure 4. The probabilities of each of the ten nodes being selected by the attacker or the defender, with strategy constraints, are compared with those without constraints when different numbers of nodes are being attacked or defended ($|V^A| = |V^D| = 2, 3, 4$).

According to Figure 4, by applying the proposed model, the selection probability of the 10 nodes in the target network changes substantially. When the number of attackable or defendable nodes is two, the change in the selection probability for different nodes is significant. However, as the number of attackable or defendable nodes increases, this change becomes less apparent. Specifically, when the number of nodes to be attacked or

defended is two, the selection probabilities V_1 and V_2 significantly increase for the attacker. For the defender, the selection probability of V_1 decreases, while the selection probability of the other nodes does not change significantly. When the number of attackable or defendable nodes is three, there is a small fluctuation in the selection probability of $V_3, V_4, V_5, \cdots, V_{10}$ for both the attacker and the defender. When the number of nodes is four, only small changes occur.

According to our experiments, we have found key insights that set apart unconstrained and constrained scenarios. Constraints significantly impact the choices of both attackers and defenders. This shows that constraints are not just theoretical; they affect real-world security strategies. Without constraints, decision makers focus on single node metrics when choosing strategies. But with constraints, they must think broadly, considering node interconnections and dependencies. This broadens the strategic landscape, mirroring the complexity of actual security situations.

5. Conclusions

Currently, infrastructure attack and defense scenarios have attracted considerable attention. The integration of complex network theory and game theory has provided valuable insights for choosing attack and defense strategies. Modeling an attacker–defender game helps in the analysis of strategic choices. To fit this to realistic situations, we propose a strategy constraint rule and a static game model under this rule.

This approach provides foundational understanding but is recognized to be a simplification of complex realities. In practice, strategic choices are subject to a multitude of constraints, including, but not limited to, resource limitations, temporal dynamics, and regulatory frameworks. The interplay of these factors requires a more integrated model. Future work will involve the development of a more adaptive algorithm. Therefore, we propose several perspectives for future research:

(1) Dynamic constraints: Real-world infrastructure systems are dynamic and constantly changing. Decision makers may face varying constraints over time due to factors such as resource availability, changes in the threat landscape, or evolving regulations. Future research may include exploring the implications of dynamic constraints on the game model and considering how decision makers adapt their strategies based on evolving constraints.

(2) Multiobjective optimization: In addition to constraints, decision makers often need to consider multiple objectives when selecting strategies for infrastructure protection. These objectives may include minimizing damage, maximizing system resilience, or optimizing resource allocation. Future research may include integrating multiobjective optimization techniques into game models to assist decision makers in selecting strategies that balance multiple competing objectives under constrained conditions.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable

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

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Brown, G.G.; Carlyle, W.M.; Salmeron, J.; Wood, K. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In *Emerging Theory, Methods, and Applications*; Informs: Catonsville, MD, USA, 2005; pp. 102–123.
2. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 53–66. [CrossRef]

3. Ezell, B.C.; Bennett, S.P.; Von Winterfeldt, D.; Sokolowski, J.; Collins, A.J. Probabilistic risk analysis and terrorism risk. *Risk Anal.* **2010**, *30*, 575–589. [CrossRef] [PubMed]
4. Brown, G.G.; Cox, L.A., Jr. How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Anal.* **2011**, *31*, 196–204. [CrossRef] [PubMed]
5. Golany, B.; Kaplan, E.H.; Marmur, A.; Rothblum, U.G. Nature plays with dice—Terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *Eur. J. Oper. Res.* **2009**, *192*, 198–208. [CrossRef]
6. Von Neumann, J.; Morgenstern, O. *Theory of Games and Economic Behavior*, 2nd rev ed.; Princeton University Press: Princeton, NJ, USA, 1947.
7. Nash, J.F. Equilibrium Points in n-Person Games. *Proc. Natl. Acad. Sci. USA* **1950**, *36*, 48–49. [CrossRef]
8. Brown, G.G.; Carlyle, W.M.; Salmern, J.; Wood, K. Defending critical infrastructure. *Interfaces* **2006**, *36*, 530–544. [CrossRef]
9. Pita, J.; Jain, M.; Marecki, J.; Ordez, F.; Portway, C.; Tambe, M.; Western, C.; Paruchuri, P.; Kraus, S. Deployed armor protection: The application of a game theoretic model for security at the los angeles international airport. In Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems: Industrial Track, Estoril, Portugal, 12–16 May 2008; pp. 125–132.
10. Zhang, L.; Reniers, G. A game-theoretical model to improve process plant protection from terrorist attacks. *Risk Anal.* **2016**, *36*, 2285–2297. [CrossRef]
11. Feng, Q.; Cai, H.; Chen, Z.; Zhao, X.; Chen, Y. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. *J. Loss Prev. Proc.* **2016**, *43*, 614–628. [CrossRef]
12. Feng, Q.; Cai, H.; Chen, Z. Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 105900. [CrossRef]
13. Zhang, X.; Ding, S.; Ge, B.; Xia, B.; Pedrycz, W. Resource allocation among multiple targets for a defender-attacker game with false targets consideration. *Reliab. Eng. Syst. Saf.* **2021**, *211*, 107617. [CrossRef]
14. Guan, P.; He, M.; Zhuang, J.; Hora, S.C. Modeling a multitarget attacker–defender game with budget constraints. *Decis. Anal.* **2017**, *14*, 87–107. [CrossRef]
15. Zhang, C.; Ramirez-Marquez, J.E. Protecting critical infrastructures against intentional attacks: A two-stage game with incomplete information. *IIE Trans.* **2013**, *45*, 244–258. [CrossRef]
16. Erdos, P.; Renyi, A. On Random Graphs I. *Publ. Math.* **1959**, *4*, 3286–3291. [CrossRef]
17. Watts, D.J.; Strogatz, S.H. Collective dynamics of 'small-world' networks. *Nature* **1998**, *393*, 440–442. [CrossRef] [PubMed]
18. Barabasi, A.L.; Albert, R. Emergence of scaling in random networks. *Science* **1999**, *286*, 509–512. [CrossRef]
19. Li, X.; Chen, G.R. A local-world evolving network model. *Phys. A Stat. Mech. Its Appl.* **2003**, *328*, 274–286. [CrossRef]
20. Comellas, F.; Ozon, J.; Peters, J.G. Deterministic small-world communication networks. *Inf. Process. Lett.* **2000**, *76*, 83–90. [CrossRef]
21. Fu, C.Q.; Gao, Y.J.; Zhong, J.L.; Sun, Y.; Zhang, P.T.; Wu, T. Attack-defense game for critical infrastructure considering the cascade effect. *Reliab. Eng. Syst. Saf.* **2021**, *216*, 107958.
22. Gu, X.Q.; Zeng, C.Y.; Xiang, F.T. Applying a Bayesian Stackelberg game to secure infrastructure system: From a complex network perspective. In Proceedings of the 2019 4th International Conference on Automation, Control and Robotics Engineering, Shenzhen, China, 19–21 July 2019; pp. 1–6.
23. Zeng, C.Y.; Ren, B.A.; Li, M.L.; Liu, H.F.; Chen, J. Stackelberg game under asymmetric information in critical infrastructure system: From a complex network perspective. *Chaos* **2019**, *29*, 083129. [CrossRef]
24. Qi, G.X.; Li, J.C.; Xu, C.; Chen, G.; Yang, K. Attack-Defense game model with multi-type attackers considering information dilemma. *Entropy* **2022**, *25*, 57. [CrossRef]
25. Qi, G.X.; Li, J.C.; Xu, X.M.; Chen, G.; Yang, K.W. An attack–defense game model in infrastructure networks under link hiding. *Chaos* **2022**, *32*, 113109. [CrossRef]
26. Huang, Y.X.; Wu, J.J.; Chi, K.T.; Zheng, Z.B. Sequential attacker–defender game on complex networks considering the cascading failure process. *IEEE Trans. Comput. Soc. Syst.* **2021**, *9*, 518–529. [CrossRef]
27. Baykal-Guersoy, M.; Duan, Z.; Poor, H.V.; Garnaev, A. Infrastructure security games. *Eur. J. Oper. Res.* **2014**, *239*, 469–478. [CrossRef]
28. Li, Y.P.; Tan, S.Y.; Deng, Y.; Wu, J. Attacker-defender game from a network science perspective. *Chaos* **2018**, *28*, 051102. [CrossRef]
29. 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]
30. Li, Y.P.; Deng, Y.; Xiao, Y.; Wu, J. Attack and defense strategies in complex networks based on game theory. *J. Syst. Sci. Complex.* **2019**, *32*, 1630–1640. [CrossRef]
31. Thompson, K.H.; Tran, H.T. Application of a defender-attacker-defender model to the US air transportation network. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018; pp. 1–5.
32. Thompson, K.H.; Tran, H.T. Operational perspectives into the resilience of the US air transportation network against intelligent attacks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 1503–1513. [CrossRef]
33. Sun, J.; Wang, S.; Zhang, J.; Dong, Q. Attack–defense game in interdependent networks: A functional perspective. *J. Infrastruct. Syst.* **2023**, *29*, 04023020. [CrossRef]

34. Li, Y.; Qiao, S.; Deng, Y.; Wu, J. Stackelberg game in critical infrastructures from a network science perspective. *Phys. A Stat. Mech. Its Appl.* **2019**, *521*, 705–714. [CrossRef]
35. 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]
36. 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]
37. Charnes, A. Constrained games and linear programming. *Proc. Natl. Acad. Sci. USA* **1953**, *39*, 639–641. [CrossRef] [PubMed]
38. Owen, G. *Game Theory*; Emerald Group Publishing: Leeds, UK, 2013.
39. Firouzbakht, K.; Noubir, G.; Salehi, M. Linearly constrained bimatrix games in wireless communications. *IEEE Trans. Commun.* **2015**, *64*, 429–440. [CrossRef]
40. Xiao, Y.; Li, D.F. Bilinear programming method for interval number bimatrix games with strategy constraints. *J. Oper. Res.* **2019**, *23*, 59–70.
41. Cohen, R.; Havlin, S. *Complex Networks: Structure, Robustness and Function*; Cambridge University Press: Cambridge, UK, 2010.
42. Latora, V.; Marchiori, M. Efficient behavior of small-world networks. *Phys. Rev. Lett.* **2001**, *87*, 198701. [CrossRef] [PubMed]
43. Bonacich, P. Factoring and weighting approaches to status scores and clique identification. *J. Math. Sociol.* **1972**, *2*, 113–120. [CrossRef]
44. Freeman, L.C. Centrality in social networks: Conceptual clarification. *Soc. Netw.* **2002**, *1*, 238–263. [CrossRef]
45. Newman, M.J. A measure of betweenness centrality based on random walks. *Soc. Netw.* **2005**, *27*, 39–54. [CrossRef]
46. Stephenson, K.; Zelen, M. Rethinking centrality: Methods and examples. *Soc. Netw.* **1989**, *11*, 1–37. [CrossRef]