entropy

Article

Attack–Defense Game Model with Multi-Type Attackers Considering Information Dilemma

Gaoxin Qi, Jichao Li *, Chi Xu, Gang Chen and Kewei Yang

College of Systems Engineering, National University of Defense Technology, Changsha 410073, China
* Correspondence: ljcnudt@hotmail.com

Abstract: Today, people rely heavily on infrastructure networks. Attacks on infrastructure networks can lead to significant property damage and production stagnation. The game theory provides a suitable theoretical framework for solving the problem of infrastructure protection. Existing models consider only the beneficial effects that the defender obtains from information gaps. If the attacker's countermeasures are ignored, the defender will become passive. Herein, we consider that a proficient attacker with a probability in the game can fill information gaps in the network. First, we introduce the link-hiding rule and the information dilemma. Second, based on the Bayesian static game model, we establish an attack–defense game model with multiple types of attackers. In the game model, we consider resource-consistent and different types of distributions of the attacker. Then, we introduce the solution method of our model by combining the Harsanyi transformation and the bi-matrix game. Finally, we conduct experiments using a scale-free network. The result shows that the defender can be benefited by hiding some links when facing a normal attacker or by estimating the distribution of the attacker correctly. The defender will experience a loss if it ignores the proficient attacker or misestimates the distribution.

Keywords: infrastructure networks protection; link hiding rule; Bayesian game; Harsanyi transformation

Citation: Qi, G.; Li, J.; Xu, C.; Chen, G.; Yang, K. Attack–Defense Game Model with Multi-Type Attackers Considering Information Dilemma. *Entropy* **2023**, *25*, 57. https://doi.org/10.3390/e25010057

Academic Editor: José F. F. Mendes

Received: 9 November 2022
Revised: 14 December 2022
Accepted: 23 December 2022
Published: 28 December 2022

1. Introduction

Critical infrastructures, such as electrical power systems, communications systems, and oil pipeline systems, exist in the form of networks and play an essential role in the lives of modern residents. Damage to these infrastructures brings tremendous economic losses and generates negative social influence. The importance of infrastructure attracts terrorists and enemies during wars. Recently, the Crimean Bridge, which undertook a resupply mission for the Russian army, was blown up, and one-third of the Ukrainian power plants were destroyed, leading to power outages across the country. The protection of infrastructure networks must be settled urgently.

Most research mainly considers the antagonism between the attacker and the defender and studies the allocation of defensive resources or the establishment of defensive strategies by building a game model suitable for the characteristics of various infrastructures. Feng et al. [1] established a static game model and Bayesian game model to analyze defense allocation for chemical facilities. Regarding the power system, Tas et al. [2] considered the cascade failure of the power grid and analyzed how the attacker harnesses it in the game. For transposition systems, Talarico et al. [3] built a framework to warn against impending attacks on the transportation infrastructure.

Combining game theory with complex networks theory, Li et al. [4–6] considered different disintegration strategies and analyzed the influence of network structure on equilibrium. Zeng et al. [7] contracted a false network to mislead an attacker by reconnecting links and studied the influence of asymmetric information on the game. They also built a Bayesian game model to solve the problem of multi-type attackers who have different payoff functions [8]. We design a link hiding rule to create the information gap between the defender and the attacker and compare the benefit of hiding links with reconnected links [9].

In previous research, there are some methods that build information gaps to mislead the attacker in game, such as hidden node information, hidden links in networks, and the construction of false links. However, the attackers can fill those gaps through reconnaissance and link predictions. In this paper, we build a Bayesian game model with a defender and an attacker to study the situation in which hidden links are discovered. We assume that there exist several types of attacker. The proficient attacker can discover the whole network structure, and the normal attacker cannot find the hidden links. In the view of the defender, the different type of attacker exists with a distribution of probability, which is prior probabilities in a Bayesian game. Then we calculate the Bayesian equilibrium in different parameter combinations. We consider the two situations of misjudgment. The result is shown that underestimating the probability of the proficient attacker is more serious.

The remainder of this paper is organized as follows: Section 2 introduces some related works; Section 3 introduces a link-hiding rule and information dilemma. Section 4 establishes an attack–defense game model based on the Bayesian static game model and presents the solution method; Section 5 shows the equilibrium results in a scale-free network and analyzes the impact of link information. Section 6 concludes this paper.

2. Related Work

Our study is related to the protection of infrastructure using game theory. Researchers have used different modeling methods and game models for different scenarios. A static game model is typically used to solve the problem of choice. The dynamic game model is suitable for situations in which offensive and defensive actions are in multiple phases and not simultaneous. A Bayesian game model is built to resolve the uncertainty problem, which can be estimated using probability distributions.

Using a static game model, Bier et al. [10] studied the reallocation of attack and defense sources. Feng et al. [1] studied how to optimize the allocation of defensive resources for multiple chemical facilities. They considered the influence of chemical materials when chemical facilities were attacked and used this influence as the measure function. Baykal-Guersoy et al. [11] considered the number of people affected or the occupancy level of critical infrastructure as a risk measure after attacking the infrastructure security game. Chen et al. [12] evaluated the performance of defense strategies using a two-person, zero-sum game model. Fu et al. [13] developed a two-person static game model for the cascade effect of the infrastructure and analyzed a pure and mixed strategy equilibrium. Li et al. [4] used the largest connected component of a network as a metric function and investigated the effect of the network structure on the equilibrium solution.

Using a dynamic game model, Baykal-Guersoy et al. [11] studied the protection of critical infrastructure in multiple stages. Brown et al. [14] established a defender–attacker model and a defender–attacker–defender game model to study homeland defense, which is a multiple-phase game. Li et al. [6] investigated the effect of the first-mover advantage on equilibrium. Fu et al. [15] first protected the network through protective or camouflaged behavior.

Using a Bayesian game model, Zhang et al. [16] classified an attacker into two types using different cost methods and analyzed how to choose defense strategies using the Bayesian Nash equilibrium. Zeng et al. [8] built a two-type attacker game model in which different attackers have different payoff functions. Feng et al. [17] studied a game for chemical facilities with multiple types of attackers, and different chemical facilities had different values for different types of attackers. Jiang et al. [18] developed a Bayesian Stackelberg game model to study the problem of water supply network protection, including four private information cases. Gu et al. [19] built a Bayesian Stackelberg game model for attackers with different utility functions and analyzed the effect of the type of distribution on the equilibrium solution.

Much research has been conducted to protect infrastructure in various scenarios using game theory. However, they ignored the situation of hiding the information being found. We proposed a link-hiding rule in a previous work, which can build an information gap in the network structure. We study the situation in which an attacker discovers hidden structural information and how to deal with it.

3. Link Hiding Rule and Information Dilemma

In this section, we introduce a link-hiding rule whose validity is proven in dynamic games. Furthermore, we consider the situation in which hidden links are discovered and analyze why the defender is influenced by the situation.

3.1. Link Hiding Rule

The link is an essential part of the network, representing various relationships between nodes, and plays the roles of transmission, transportation, and transformation. The importance of the links and nodes is interrelated. For example, when a node has more links, its degree centrality is high. Simultaneously, a link connecting two nodes with higher degrees is more important. There are several ways to change a network's structure, such as reconnecting links [20] and adding links [21]. To reduce the damage to principal targets by attackers as much as possible, we assume that the probability of a hidden link connection is positively related to the properties of the nodes on both sides of the link. The number of hidden links depended on the network structure.

Infrastructure networks can be presented as a simple undirected graph $G = (V, E)$, where $V = [v_1, v_2, \ldots, v_N]$ represents the node set, and $E = (e_{ij})_M \subseteq V \times V$ represents the link set. The number of nodes and links are $N = |V|$ and $M = |E|$, respectively. Let $A(G) = (a_{ij})_{N\times N}$ represent the adjacency matrix of graph G. $a_{ij} = a_{ji} = 1$ if a link exists between v_i and v_j; otherwise, $a_{ij} = a_{ji} = 0$. Let $r_i > 0$ represent the properties of nodes, for example, the degree, betweenness, or capability of nodes. Sorting $\{r_i\}_N$ in the descending order, we obtain $r_{(1)} \geq r_{(2)} \geq \cdots \geq r_{(N)}$. Let k_i represent the degree of the node v_i. Then the weighted average of r_i can be defined as $\bar{r} = \frac{\sum_{i=1}^{N} k_i r_i}{\sum_{i=1}^{N} k_i}$.

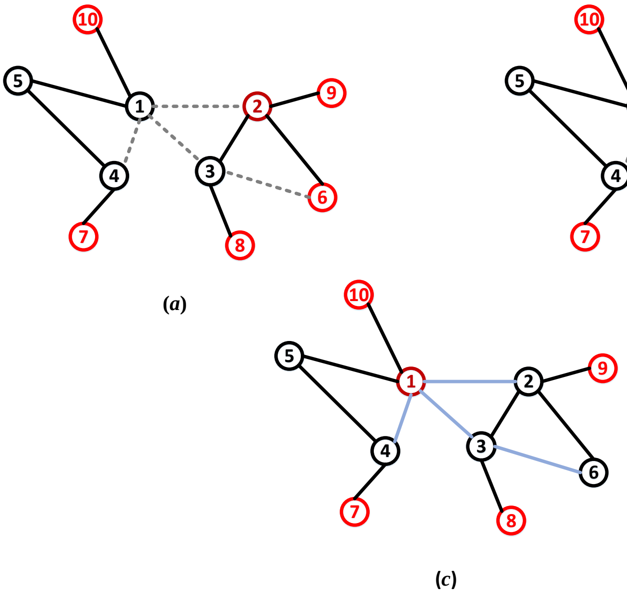
We design the sum of hidden links as αM and define the hidden probability of the link as p_{ij} associated with the property of node v_i and v_j, then p_{ij} can be represented as:

$$p_{ij} = \alpha M \frac{r_i + r_j}{\sum_{i=1}^{N} k_i r_i} \tag{1}$$

where $\alpha \in [0, \frac{2}{r_{(1)}+r_{(2)}}\bar{r}]$ is called the average hiding coefficient. $\sum p_{ij} = \alpha M$.

3.2. Information Dilemma

In cities, communication and power cables exist in the form of burial [22]. This creates the conditions for hiding some of the links. The defender can mislead the attacker's strategy choices by hiding a part of the link. For example, from the attacker's perspective, the node's highest degree is 2 in Figure 1a after hiding links, and the lowest degree of nodes is 6, 7, 8, 9, and 10. This value deviates from the actual value. In addition, it is assumed that a node with five degrees is destroyed, requiring five units of offensive recourse. Then, Nodes 2 and 6 are attacked with unsaturated resources, which may lead to attack failure. Hiding links is not always effective. An attacker can find hidden links by scouting or link prediction. As shown in the figure, the attack strategies vary with different network topology information. Attackers are classified based on their level of information. We refer to the type of attacker in Figure 1a as the normal type, the type in Figure 1b as the semi-proficient type, and the type in Figure 1c as the proficient type. The network after hiding links is called a misleading network.



(*a*) (*b*)

(*c*)

Figure 1. The networks structure information held by different types of attackers, (**a**) normal attacker, (**b**) semi-proficient attacker, (**c**) proficient attacker. The gray dotted line represents the hidden link, and the blue line represents the hidden link discovered by the attacker.

The link hiding creates a dilemma for the defender facing multi-type attackers. On the one hand, link hiding can benefit the defender by misleading the normal attacker. On the other hand, link hiding will bring loss to the defender who does not effectively deal with the proficient attacker. The dilemma is built by the information on network structure. To defuse the attack, the defender adapts the optimal reaction strategy to the attack strategy as the defense strategy. The attack strategies change with the attacker's topology information, which is uncertain to the defender.

4. The Attack–Defense Game Model with Multi-Type Attackers under Information Dilemma

Considering the information dilemma caused by hidden links, we built a static game model based on Bayesian games. The type of attacker is uncertain, but the defender can estimate the distribution of the type. To simplify the model, we consider the proficient and normal types of attacker, and the distribution is estimated to $\Omega = (\omega, 1-\omega)$.

4.1. Cost Model

We considered only the strategy of the node here. When a node is removed, the links are removed. The source of the attack and defense node v_i is denoted by c_i, a parameter related to the node's property r_i:

$$c_i = r_i, \tag{2}$$

Assuming that the resources of attack or defense for all nodes are $\widetilde{C}$, then:

$$\widetilde{C} = \sum_{i=1}^{N} c_i = \sum_{i=1}^{N} r_i, \tag{3}$$

we donate $\theta^A \in [0,1]$ as the cost constraint coefficient, the attacker's available resources can be represented as $\widetilde{T}^A = \theta^A \widetilde{C}^A = \theta^A \sum_{i=1}^{N} r_i^{\beta}$. Similarly, we can define $\widetilde{C}^D$ and $\widetilde{T}^D$ by $\widetilde{C}^D = \sum_{i=1}^{N} c_i^D = \sum_{i=1}^{N} (r_i)$, and $\widetilde{T}^D = \theta^D \widetilde{C}^D = \theta^D \sum_{i=1}^{N} r_i$, respectively.

The $d = (d_1, d_2, \ldots, d_N) \in S_D$ is donated as a defensive strategy satisfying resource constraints, where S_D is the strategy set of the defender. If the node is defended, we have $d_i = 1$; otherwise, $d_i = 0$. The cost of d is:

$$C_d^D = \sum_{v_i \in V^D} r_i = \sum_{i=1}^{N} d_i r_i \leq \widetilde{T}^D = \theta^D \sum_{i=1}^{N} r_i. \tag{4}$$

Similarly, we can define the attacker's cost C_a^A, where $a = [a_1, a_2, \ldots, a_N] \in S_A$:

$$C_a^A = \sum_{v_i \in V^A} r_i = \sum_{i=1}^{N} a_i r_i \leq \widetilde{T}^A = \theta^A \sum_{i=1}^{N} r_i. \tag{5}$$

We note that r_i of the same nodes might be different for the attacker and defender. When links are hidden, r_i is changed in the infrastructure networks, which means a cost change. Insufficient attacks may not damage the nodes. Let V^A represent the set of attacked nodes. We define the success rates to reflect this effect: $\forall v_i \in V^A$

$$ps_i = \begin{cases} 0 & \text{if } \frac{c_i^A - c_i^D}{r_i} < 0 \\ \frac{c_i^A - c_i^D}{r_i} & \text{if } 0 \leq \frac{c_i^A - c_i^D}{r_i} \leq 1 \\ 1 & \text{if } 1 < \frac{c_i^A - c_i^D}{r_i}. \end{cases} \tag{6}$$

where r_i^A and r_i^D represent the node properties in the views of the attacker and defender, respectively. Here, r_i is the degree of the nodes.

4.2. Strategy Set

Here, we only consider two typical strategies:

(1) High-degree attack or defense strategy. A high-degree attack strategy damages nodes with a high degree. The high-degree defense strategy defends nodes with a high degree.

(2) Low-degree attack or defense strategy. The low-degree attack strategy is aimed at nodes with a low degree. Because the resources consumed are relatively low compared with high-degree nodes, the low-degree attack at the same cost can destroy more low-degree nodes. The low-degree defense strategy defends nodes with a low degree.

Specifically, the attacker develops strategies based on the network structure it owns. A proficient attacker adopts a strategy based on the true network, and thus it has a high-degree attack strategy in true networks (THA) and a low-degree attack strategy in true networks (TLA). A normal attacker adopts a high-degree attack strategy in misleading networks (MHA) and a low-degree attack strategy in misleading networks (MLA). As the best response strategies, defenders need to consider four strategies: high-degree defense strategy in true networks (THD), low-degree defense strategy in true networks (TLD), high-degree defense strategy in misleading networks (MHD), and low-degree defense strategy in misleading networks (MLD).

4.3. Payoff Function

We denote the measure function of the network performance by Γ, including the efficiency and size of the largest connected component. Let $\widehat{G}$ represent the network after a game round. Then, the defender's payoff function is

$$u^D(a, d) = \frac{\Gamma(\widehat{G}) - \Gamma(G)}{\Gamma(G)}. \tag{7}$$

Similarly, the payoff of the attacker can be defined as:

$$u^A(a, d) = \frac{\Gamma(G) - \Gamma(\widehat{G})}{\Gamma(G)}. \tag{8}$$

Here the G might be different between Equations (7) and (8) for partly hiding links.

5. Solution Method

The Bayesian Nash equilibrium is a general solution for the Bayesian game model, and we used it as the solution here. The solution form is ((the equilibrium of type 1 of the attacker, the equilibrium of type 2 of the attacker), the equilibrium of the defender). Let the distributions of the defender's strategy and the attacker's strategy be $P = (p_1, p_2, \ldots, p_n)'$ and $Q_k = (q_1^{a_k}, q_2^{a_k}, \ldots, q_{m^{a_k}}^{a_k})' \in [0,1]^{m^{a_k}}$, where n and m^{a_k} represent the number of defender's and $k-th$ type of attacker's strategies, respectively. The attacker's objective function can be donated as:

$$\max O^{a_k} = \max P' U^{a_k} Q_k, \tag{9}$$

where U^{a_k} represents the payoff matrix of the $k-th$ type of attacker.

The defender's objective function can be denoted as follows:

$$\max O^d = \max \sum_{k=1}^{K} \omega_k P' U^d Q_k, \tag{10}$$

where U^d represents the payoff matrix of the defender.

The attack–defense game model established here is a Bayesian static game model in which both attackers and defenders act simultaneously. In other words, before the game occurs, neither the attacker nor the defender knows which strategy the other side has adopted. The Bayesian static game model can be transformed into a complete information static game model using Harsanyi transformation [23]. The solution of the Bayesian static game model is defined as the Bayesian Nash equilibrium (BNE). Let the solution be of the form $(P^*, Q_1^*, Q_2^*, \ldots, Q_K^*)$ Then, we have:

$$P^{*\prime} U^{a_k} Q_k^* \geq P^{*\prime} U^{a_k} Q_k \tag{11}$$

$$\sum_{k=1}^{K} \omega_k P^{*\prime} U^{a_k} Q_k^* \geq \sum_{k=1}^{K} \omega_k P' U^{a_k} Q_k^* \tag{12}$$

Specifically, we considered a payoff matrix for two types of attackers. When the attacker is normal, the attacker does not have full information about the network structure. At this point, it creates strategies and calculates the payoff according to the misleading network. When the defender adopts THD and TLD, the attacker views them as MHD and MLD to calculate the payoff. When the attacker is proficient, it has full information about the entire game and knows all the strategies the defender may adopt. The payoff at this time is the value both parties calculated based on the real network. Then we can calculate the payoff matrices based on payoff function, and payoff matrices of proficient and normal attacker are shown in Tables 1 and 2, respectively.

Table 1. The payoff matrix of proficient attacker, whose probability is ω.

Type	**Proficient Attacker** (ω)	
Strategy	$\boldsymbol{THA}$	$\boldsymbol{TLA}$
THD	$u_{11}^{d_1}, u_{11}^{a_1}$	$u_{12}^{d_1}, u_{12}^{a_1}$
TLD	$u_{21}^{d_1}, u_{21}^{a_1}$	$u_{22}^{d_1}, u_{22}^{a_1}$
MHD	$u_{31}^{d_1}, u_{31}^{a_1}$	$u_{32}^{d_1}, u_{32}^{a_1}$
MLD	$u_{41}^{d_1}, u_{41}^{a_1}$	$u_{42}^{d_1}, u_{42}^{a_1}$

Table 2. The payoff matrix of normal attacker, whose probability is $1 - \omega$.

Type	**Normal Attacker $(1 - \omega)$**	
Strategy	$\boldsymbol{MHA}$	$\boldsymbol{MLA}$
THD	$u_{11}^{d_2}, u_{31}^{a_2}$	$u_{12}^{d_2}, u_{32}^{a_2}$
TLD	$u_{21}^{d_2}, u_{41}^{a_2}$	$u_{22}^{d_2}, u_{42}^{a_2}$
MHD	$u_{31}^{d_2}, u_{31}^{a_2}$	$u_{32}^{d_2}, u_{32}^{a_2}$
MLD	$u_{41}^{d_2}, u_{41}^{a_2}$	$u_{42}^{d_2}, u_{42}^{a_2}$

Based on the Harsanyi model [24,25], we can turn it to Table 3. We can solve this bi-matrix game using linear programming [26].

Table 3. The payoff matrix after the Harsanyi transformation.

Strategy	$\boldsymbol{THA, MHA}$	$\boldsymbol{THA, MLA}$	$\boldsymbol{TLA, MHA}$	$\boldsymbol{TLA, MLA}$
THD TLD MHD MLD	$\omega u^{d_1} + (1 - \omega)u^{d_2}, \omega u^{a_1} + (1 - \omega)u^{a_2}$			

6. Experiments

Most real-world networks are scale-free, such as airplane networks [27] and bank payoff networks [28]. We used the Barabási–Albert model to construct a scale-free network with 300 nodes and an average degree of 2. We conducted 500 independent experiments based on this network and obtained the average payoff. Main definitions used in this section are shown in Table 4.

Table 4. Abbreviations and definitions.

Abbreviations	**Definitions**
BNE	Bayesian Nash equilibrium
TN	True network
MN	Misleading network
THA	High-degree attack strategy based on true networks
TLA	Low-degree attack strategy based on true networks
MHA	High-degree attack strategy based on misleading networks
MLA	Low-degree attack strategy based on misleading networks
THD	High-degree defense strategy based on true networks
TLD	Low-degree defense strategy based on true networks
MHD	High-degree defense strategy based on misleading networks
MLD	Low-degree defense strategy based on misleading networks
MD	Strategy set contains MHD and MLD
MA	Strategy set contains MHA and MLA

6.1. Benefits of the Link Hiding for the Defender

The degree values of the nodes with different link hidden coefficients are shown in Figure 2. According to the figure, the height degree of the node decreases more than the low degree of the nodes, with an increase in the average link hiding coefficient. Hiding some links disturbs the order of the degrees. The high-degree attack strategy based on a misleading network excludes some nodes, although its degree is high in reality.

If the link hiding cannot improve the defender's payoff in any situation, an information dilemma does not exist. We prove the benefit to the defender facing the normal attacker by partly hiding links. Facing a normal attacker, ω equals zero, and the game degenerates into a complete information game. We calculate the payoff of the Nash equilibrium when applying MD (the strategy set contains MHD and MLD) against MA (the strategy set contains MHA and MLA), and the results are shown in Figure 3. We found that hidden links can benefit the defender and that the benefit to the defender increases with an increase in the link hidden coefficient.

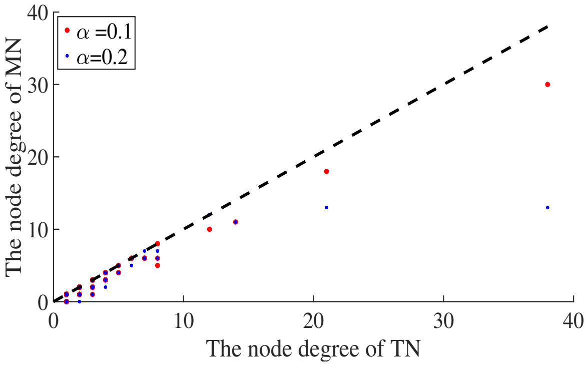


Figure 2. The degree value of the node in the true network (TN) and the misleading network (MN). The x-axis represents the true degree value of the node, and the y-axis represents the degree value of the node behind the hidden link. The red and blue dots represent the change in the degree value of the node when the link hidden coefficient $\alpha = 0.1$ and $\alpha = 0.2$, respectively.

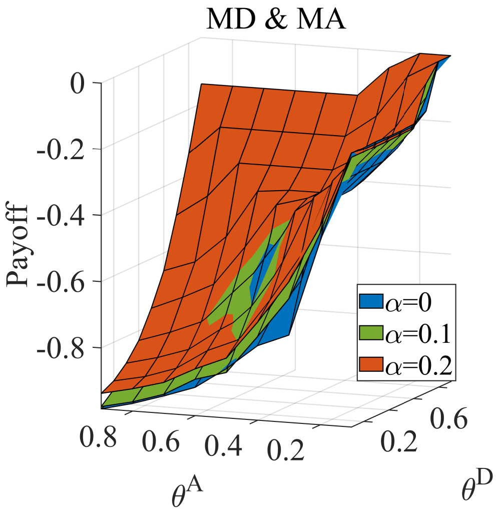


Figure 3. The defender's equilibrium payoff when the defender adopts the MD set facing the normal attacker, when attack cost constraint coefficient $\theta^A \in [0.1, 0.9]$, defense cost constraint coefficient $\theta^D \in [0.1, 0.9]$, average link hiding coefficient $\alpha = 0, 0.1, 0.2$.

We computed the Bayesian Nash equilibrium of the defender when the distributions of the attacker type $\Omega = (\omega, 1 - \omega)$ were $(0.1, 0.9)$, $(0.5, 0.5)$, $(0.7, 0.3)$. The results are shown in Figure 4. According to the figure, the probability of the defender adopting the real strategy gradually increases with a gradual increase in the number of hidden links and the probability of a highly proficient attacker. We observed that when the probability of a proficient attacker is low, the defender still adopts TD (the defense strategies based on the true network) in some cases, particularly THD (the high-degree defense strategy based on the true network). TD covers more real critical nodes and allocates more resources to protect the network. The defender adopts MD (the defense strategies based on a misleading network), which can better cope with the normal attacker when the defender's cost constraint coefficient and the probability of the proficient attacker are both low. The MD cost is lower than TD. We also calculated the defender's equilibrium payoff; the results are shown in Figure 5. As seen in Figure 5, the defender's payoff increases as the defense cost increases and the attack cost decreases. Hiding partial links can benefit the defender in most situations in the Bayesian Nash equilibrium. There are also singularities when the probability of a proficient attacker is high.

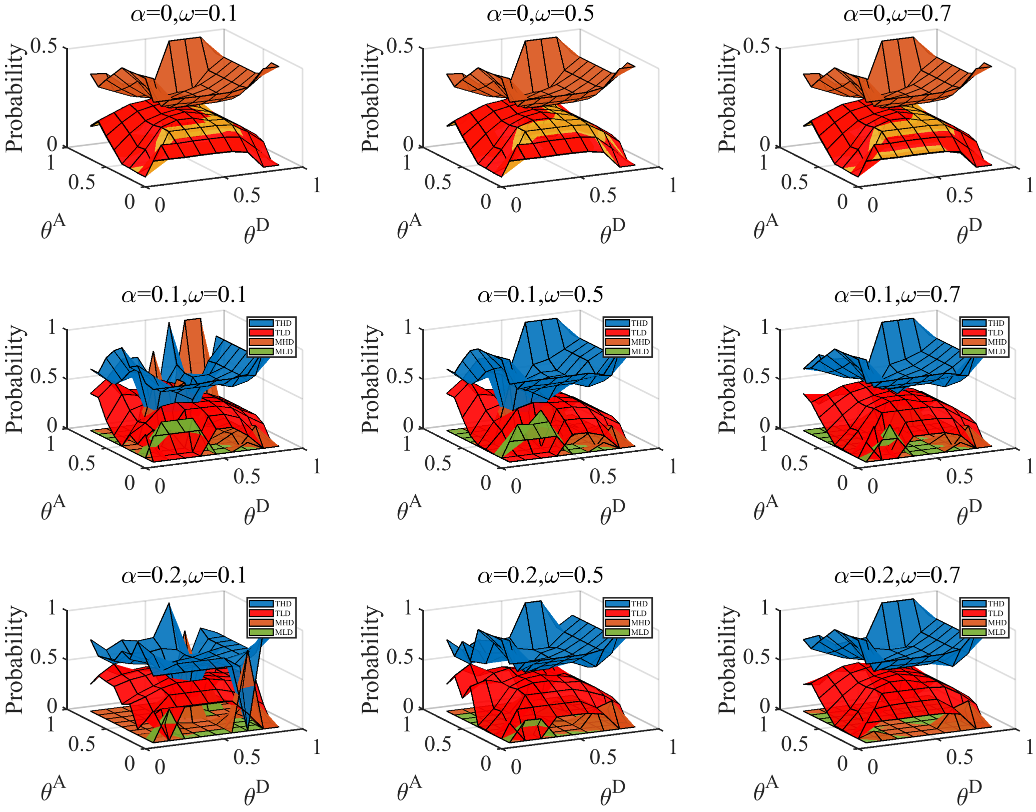


Figure 4. Probabilities of the defender's strategies in Bayesian Nash equilibrium under different attack cost constraint coefficient θ^A and defense cost constraint coefficient combinations, when average link hiding coefficient $\alpha = 0, 0.1, 0.2$, probability of the proficient attacker ω equal $0.1, 0.5, 0.7$. The yellow grid represents when TLD and MLD coincide.

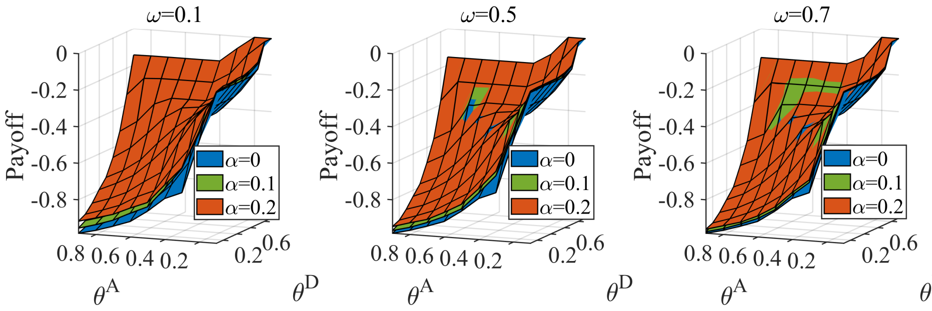


Figure 5. Defender's equilibrium payoff under different attack cost constraint coefficient θ^A and defense cost constraint coefficient θ^D combinations, when average link hiding coefficient $\alpha = 0, 0.1, 0.2$, probability of the proficient attacker ω equal $0.1, 0.5, 0.7$.

6.2. Equilibrium with Different Distributions of the Attacker's Type

The attacker is the proficient type, and its equilibrium strategy is shown in Figure 6. When the attacker has more resources than the defender, it adopts the high-degree strategy to attack the critical nodes, which cannot be covered by the high-degree defense strategy for the low-defense resource. When the defender estimates the probability of a proficient attacker as low, the defender mainly copes with the attack strategy based on the misleading network. Therefore, the proficient attacker will likely use high-degree strategies, which can obtain more payoff for destroying critical nodes. With the increase in the average hiding coefficient, the gap between the strategy based on the true network and the strategy based on the misleading network increases. The proficient attacker obtains more payoff by increasing the probability of the high-degree attack strategy. When the defender estimates the probability of a proficient attacker increase, the defender mainly resists the attack strategies based on the true network. The defender protects the critical nodes with a high-degree defense strategy. The proficient attacker decreases the probability of the high-degree strategy to avoid defense.

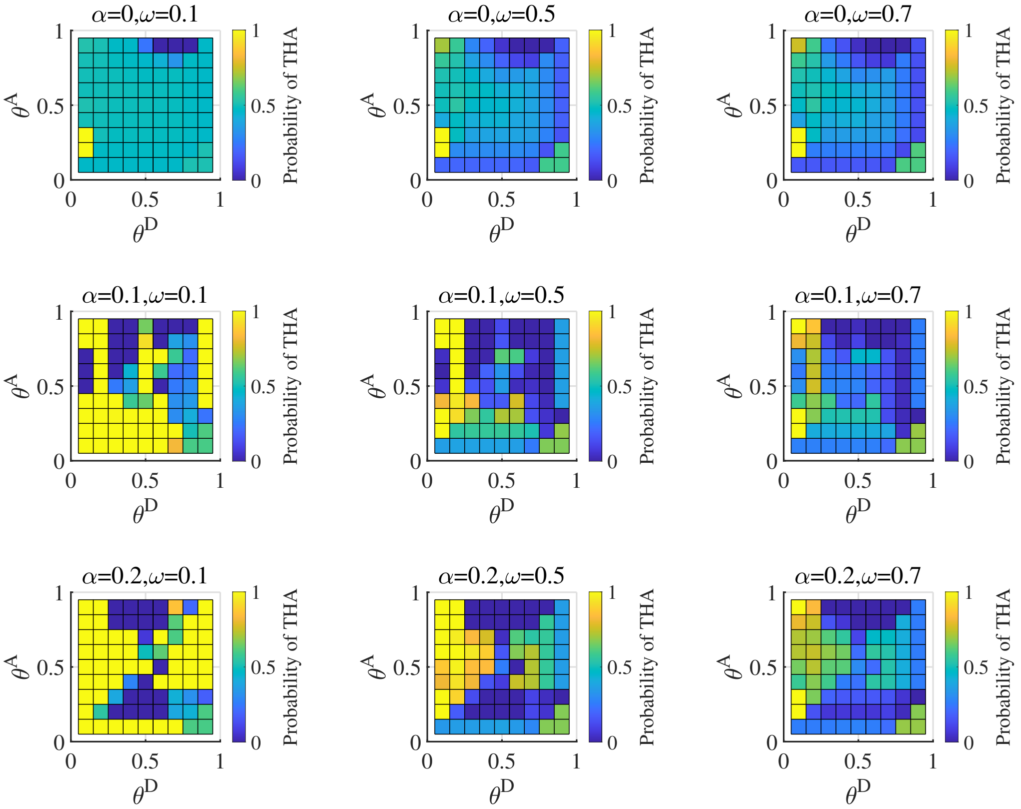


Figure 6. Probability of the proficient attacker adopting high-degree attack strategies based on the true network under different attack cost constraint coefficient ($\theta^A \in [0.1, 0.9]$) and defense cost constraint coefficient ($\theta^D \in [0.1, 0.9]$) combinations in Bayesian Nash equilibrium, when average hiding coefficient $\alpha = 0, 0.1, 0.2$, probability of the proficient attacker $\omega = 0.1, 0.5, 0.7$.

When the attacker is of the normal type, the equilibrium strategy is shown in Figure 7. The normal attacker has a similar result to the proficient attacker. When the probability of the normal type is high ($1 - \omega = 0.9$), the defender pays more attention to strategies based on the misleading network. Link hiding has almost no effect on the equilibrium at this time. With the decrease in the probability of the normal type, attack strategies based on the misleading network cannot be held back, and the normal attacker adopts the pure strategies. However, our calculation of the equilibrium payoff is insignificant. A normal attacker may not adopt the strategy distribution we provided. According to the Nash equilibrium definition, when the attacker adopts other strategy distributions, the payoff obtained is less than or equal to the equilibrium payoff.

6.3. Influence of the Misjudgment on the Defender

Consider the first information dilemma, in which the defender ignores the existence of the proficient attacker. When the attacker is a proficient type, and the defender does not know it at all, we calculate $u^D(THA, MHD)$ and $u^D(TLA, MLD)$ when $\alpha = 0, 0.1, 0.2$ and $\theta = \theta^A = \theta^D$, and the result is shown in Figure 8. At this moment, the defender and attacker have the same cost constraint coefficient. The gap between the corresponding "optimal response strategy" gradually increases with the link hiding coefficient. We also calculate the equilibrium payoff for this situation. The results are shown in Figure 9. This information gap reduces the defender's payoff.

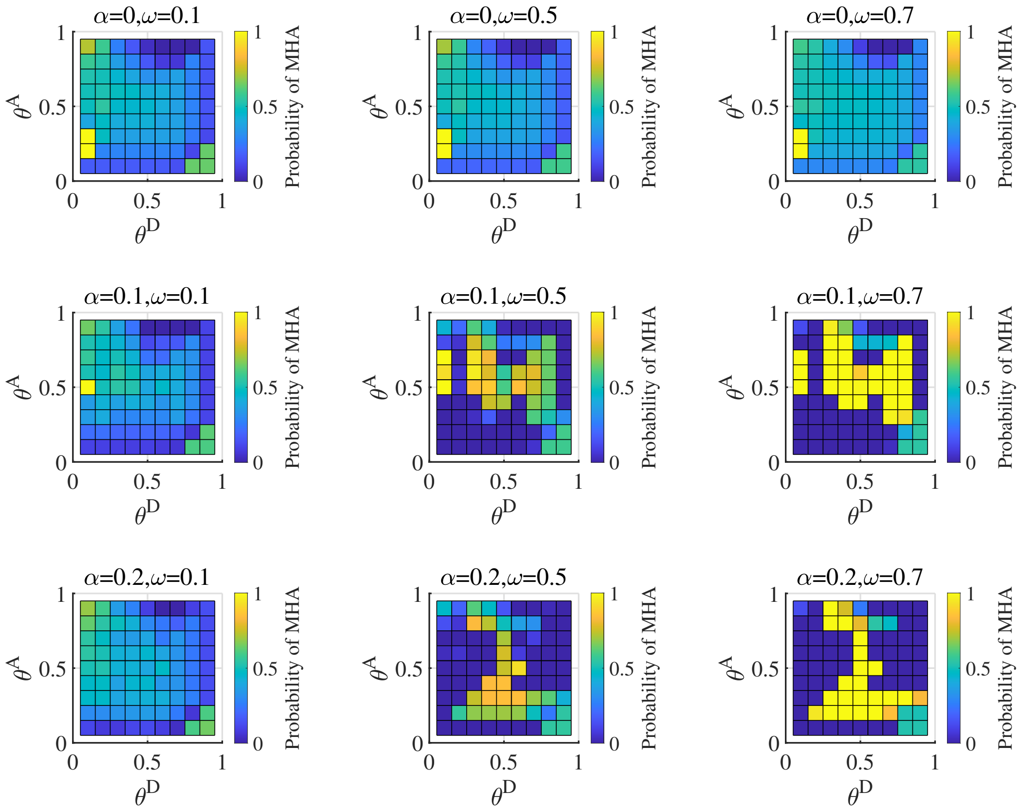
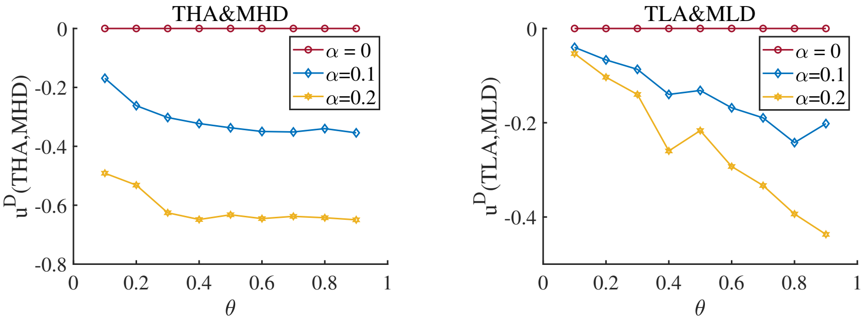


Figure 7. Probability of the normal attacker adopting MHA (the high-degree attack strategy based on the misleading network) in Bayesian Nash equilibrium under different attack cost constraint coefficient ($\theta^A \in [0.1, 0.9]$) and defense cost constraint coefficient ($\theta^D \in [0.1, 0.9]$) combinations, when average hiding coefficient $\alpha = 0, 0.1, 0.2$, probability of the normal attacker $1 - \omega = 0.9, 0.5, 0.3$.



(**a**) $u^D(THA, MHD)$ (**b**) $u^D(TLA, MLD)$

Figure 8. Payoff $u^D(THA, MHD)$ and payoff $u^D(TLA, MLD)$ when the average hiding coefficient $\alpha = 0, 0.1, 0.2$ and cost coefficient $\theta = \theta^A = \theta^D \in [0.1, 0.9]$. The THA represents the high-degree attack strategy based on the true network, and the TLA represents the low-degree attack strategy based on the true network. The MHD represents the high-degree defense strategy based on the misleading network, and the MLD represents the low-degree defense strategy based on the misleading network. The Subfigure (**a**) reflect the gap between THA and MHD, and the Subfigure (**b**) reflect the gap between TLA and MLD. Gaps increases when the α increases, which means the defender cannot cope with the attacker although it chooses right defense mode.

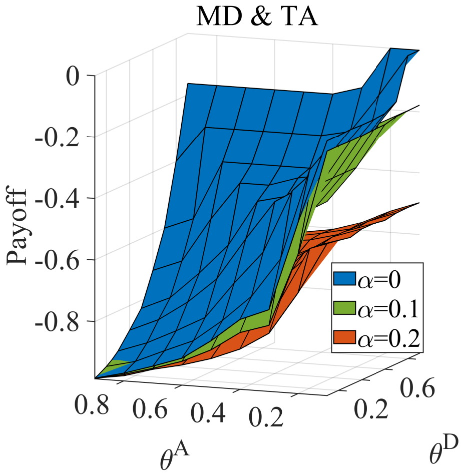


Figure 9. Defender's equilibrium payoff when the defender adopts *MHD* (high-degree defense strategy based on the misleading network) and *MLD* (low-degree defense strategy based on the misleading network) facing a proficient attacker under different attack cost constraint coefficient ($\theta^A \in [0.1, 0.9]$) and defense cost constraint coefficient ($\theta^D \in [0.1, 0.9]$) combinations.

Second, we considered the information dilemma triggered by the misjudgment of the distribution of attacker types. The defender's judgment of the type of attacker is also based on data experience and other methods. There is uncertainty in this method; therefore, there is a situation in which the attacker may be misled about the distribution. We calculate the payoff when the true type distribution is $\Omega = (0.1, 0.9)$, the misjudgment distribution is $\Omega' = (0.9, 0.1)$, the true type distribution is $\Omega = (0.9, 0.1)$ and the misjudgment distribution is $\Omega' = (0.1, 0.9)$. The results are shown in Figures 10 and 11.

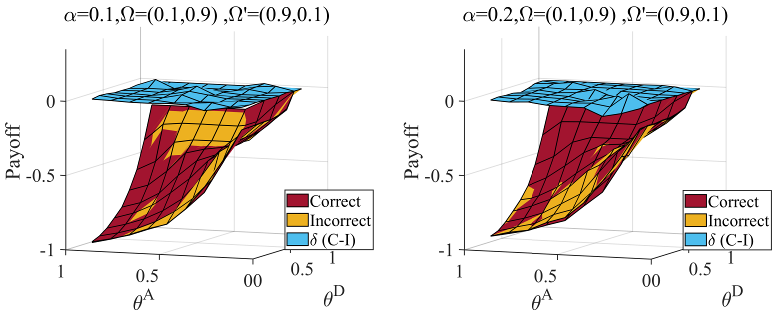


Figure 10. Defender's payoff with correct ($\Omega = (0.1, 0.9)$) and incorrect ($\Omega' = (0.9, 0.1)$) judge attacker probability distributions, when attack cost constraint coefficient $\theta^A \in [0.1, 0.9]$, defense cost constraint coefficient $\theta^D \in [0.1, 0.9]$, average hiding coefficient $\alpha = 0.1, 0.2$. The $\delta(C - I)$ represents the payoff difference between correct and incorrect situation. Link hiding brings about a loss to the defender when underestimating normal attackers.

As shown in Figure 10, in the face of the first type of misjudgment, the defender's payoff decreases in most cases, and the decrease in the payoff increases with an increase in the link hidden coefficient. There are also some singularities in this situation. When the average hiding coefficient α is equal to 0.1 and the defense cost coefficient θ^D is greater than 0.5, the payoff of incorrect judgment is greater than that of correct judgment for protecting critical nodes. With an increase in the average hiding coefficient, the degree of high-degree nodes decreases, which can be contained in a high-degree strategy based on misleading networks at a lower cost. Thus, when the average hiding coefficient α equals 0.2, the singularities appear at θ^D lower than 0.5.

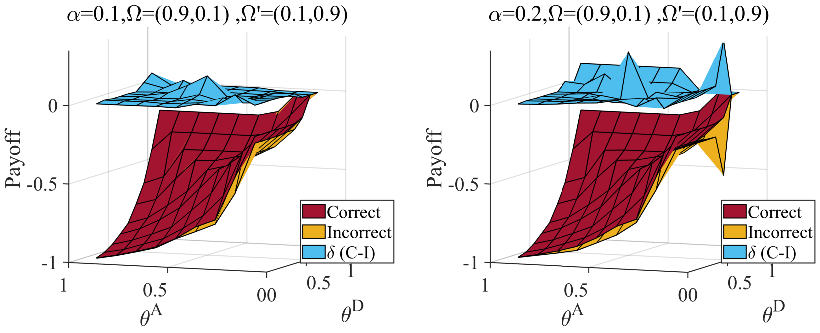


Figure 11. Defender's payoff when correct ($\Omega = (0.9, 0.1)$) and incorrect ($\Omega' = (0.1, 0.9)$) judge attacker probability distributions, attack cost constraint coefficient $\theta^A \in [0.1, 0.9]$, defense cost constraint coefficient $\theta^D \in [0.1, 0.9]$, and average hiding coefficient $\alpha = 0.1, 0.2$. The $\delta(C - I)$ represent the payoff difference between correct and incorrect situation. Link hiding brings about a loss to the defender when underestimating proficient attackers.

From Figure 11, we can obtain similar conclusions when $\Omega = (0.9, 0.1)$ and $\Omega' = (0.1, 0.9)$. An incorrect estimation can result in extra loss for hiding partial links. The loss increases with an increase in the average hiding coefficient. Combined with Figures 10 and 11, the loss of the underestimated the probability of the proficient attacker is more than that of the underestimated normal attacker.

7. Conclusions

Technology has facilitated the construction of infrastructure networks and has brought great convenience to people's lives, making residents increasingly dependent on them. To effectively protect the infrastructure network, it is necessary to combine game theory and complex network theory to study this problem. The link information plays important roles for the game participants as an essential part of infrastructure networks. The link hiding can benefit the defender facing normal attackers by building information gaps. However, when facing a proficient attacker, it causes trouble for the defender. We call the situation an information dilemma.

In this paper, we study the information dilemma by establishing a Bayesian game model. First, we introduce the link hiding rule, which is an effective method to build an information gap, and translate why the information dilemma exists. Second, we build a Bayesian game model with a multi-type of attacker. Then, we introduce the solution method. Finally, we experiment in a scale-free network. The result is shown that link hiding benefits the defender when facing the normal attacker. By the Bayesian Nash equilibrium, the defender copes with the different types of attacker and benefits by partly hiding links. We also analyze the situation of missed and incorrect judgments, which proves disadvantageous in link hiding. We should pay more attention to the proficient attacker.

Only two typical strategies are considered in our model, and more possible strategies will be considered in future work. In addition, the game model that we established mainly faces perfect rational participants. In reality, people are not always completely rational [29]. Therefore, the bounded rational groups should be studied in the future. We will make the game model more practical in the following work.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/e25010057/s1.

Author Contributions: Conceptualization, G.Q. and J.L.; methodology, G.Q. and J.L; software, G.Q.; validation, G.Q., J.L. and C.X.; formal analysis, G.Q., G.C. and J.L.; investigation, J.L. and K.Y.; writing, original draft preparation, G.Q., J.L. and C.X.; writing, review and editing, G.Q., J.L., C.X., G.C. and K.Y.; visualization, G.Q. and J.L.; project administration, G.Q.; funding acquisition, J.L. and K.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the National Natural Science Foundation of China under Grant Nos 72001209, 72231011, 71971213, 72071206 and the Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province under Grant Nos 2020RC4046, and the Science Foundation for Outstanding Youth Scholars of Hunan Province No.2022JJ20047.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article or Supplementary Materials.

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. 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. Process. Ind.* **2016**, *43*, 614–628. [CrossRef]
2. Tas, S.; Bier, V.M. Addressing vulnerability to cascading failure against intelligent adversaries in power networks. *Energy Syst.* **2016**, *7*, 193–213. [CrossRef]
3. Talarico, L.; Reniers, G.; Sörensen, K.; Springael, J. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. *Reliab. Eng. Syst. Saf.* **2015**, *138*, 105–114. [CrossRef]
4. Li, Y.; Tan, S.; Deng, Y.; Wu, J. Attacker-defender game from a network science perspective. *Chaos Interdiscip. J. Nonlinear Sci.* **2018**, *28*, 051102. [CrossRef]
5. Li, Y.; 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]
6. 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]
7. Zeng, C.; Ren, B.; Li, M.; Liu, H.; Chen, J. Stackelberg game under asymmetric information in critical infrastructure system: From a complex network perspective. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 083129. [CrossRef]
8. Zeng, C.; Ren, B.; Liu, H.; Chen, J. Applying the bayesian stackelberg active deception game for securing infrastructure networks. *Entropy* **2019**, *21*, 909. [CrossRef]
9. Qi, G.; Li, J.; Xu, X.; Chen, G.; Yang, K. An attack–defense game model in infrastructure networks under link hiding. *Chaos Interdiscip. J. Nonlinear Sci.* **2022**, *32*, 113109. [CrossRef]
10. Bier, V.; Oliveros, S.; Samuelson, L. Choosing what to protect: Strategic defensive allocation against an unknown attacker. *J. Public Econ. Theory* **2007**, *9*, 563–587. [CrossRef]
11. Baykal-Guersoy, M.; Duan, Z.; Poor, H.V.; Garnaev, A. Infrastructure security games. *Eur. J. Oper. Res.* **2014**, *239*, 469–478. [CrossRef]
12. Chen, P.; Cheng, S.; Chen, K. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.* **2012**, *50*, 24–29. [CrossRef]
13. Fu, C.; Gao, Y.; Zhong, J.; Sun, Y.; Pengtao, Z.; Wu, T. Attack-defense game for critical infrastructure considering the cascade effect. *Reliab. Eng. Syst. Saf.* **2021**, *216*, 107958.
14. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending critical infrastructure. *Interfaces* **2006**, *36*, 530–544. [CrossRef]
15. 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.
16. Zhang, H.; Dingkun, Y.U.; Wang, J.; Han, J.; Wang, N. Security Defence Policy Selection Method Using the Incomplete Information Game Model. *China Commun.* **2015**, *9*, 2.
17. 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]
18. Jiang, J.; Liu, X. Bayesian Stackelberg game model for water supply networks against interdictions with mixed strategies. *Int. J. Prod. Res.* **2021**, *59*, 2537–2557. [CrossRef]
19. Gu, X.; Zeng, C.; Xiang, F. Applying a Bayesian Stackelberg game to secure infrastructure system: From a complex network perspective. In Proceedings of the 2019 4th International Conference on Automation, Control and Robotics Engineering, Shenzhen, China, 19–21 July 2019; pp. 1–6.
20. Li, Y.; Wu, J.; Zou, A. Effect of eliminating edges on robustness of scale-free networks under intentional attack. *Chin. Phys. Lett.* **2010**, *27*, 068901.
21. Hayashi, Y.; Matsukubo, J. Improvement of the robustness on geographical networks by adding shortcuts. *Phys. A Stat. Mech. Its Appl.* **2007**, *380*, 552–562. [CrossRef]
22. Zhou, X.; Chen, Q.; Lyu, S.; Chen, H. Mapping the Buried Cable by Ground Penetrating Radar and Gaussian-Process Regression. *IEEE Trans. Geosci. Remote. Sens.* **2022**, *60*, 1–12. [CrossRef]
23. Harsanyi, J.C.; Selten, R. A generalized Nash solution for two-person bargaining games with incomplete information. *Manag. Sci.* **1972**, *18*, 80–106. [CrossRef]

24. Harsanyi, J.C. Games with incomplete information played by "Bayesian" players, I–III Part I. The basic model. *Manag. Sci.* **1967**, *14*, 159–182. [CrossRef]
25. Harsanyi, J.C. Games with incomplete information played by "Bayesian" players part II. Bayesian equilibrium points. *Manag. Sci.* **1968**, *14*, 320–334. [CrossRef]
26. Bilò, V.; Fanelli, A. Computing exact and approximate Nash equilibria in 2-player games. In *Proceedings of the International Conference on Algorithmic Applications in Management*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 58–69.
27. De Masi, G.; Iori, G.; Caldarelli, G. Fitness model for the Italian interbank money market. *Phys. Rev. E* **2006**, *74*, 066112. [CrossRef] [PubMed]
28. Guimera, R.; Mossa, S.; Turtschi, A.; Amaral, L.N. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proc. Natl. Acad. Sci. USA* **2005**, *102*, 7794–7799. [CrossRef] [PubMed]
29. Zhang, J.; Wang, Y.; Zhuang, J. Modeling multi-target defender-attacker games with quantal response attack strategies. *Reliab. Eng. Syst. Saf.* **2021**, *205*, 107165. [CrossRef]

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