Computing Effective Mixed Strategies for Protecting Targets in Large-Scale Critical Infrastructure Networks

Zhen Wang, Mengting Jiang, Yu Yang, Lili Chen and Hong Ding*

School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China

Most critical infrastructure networks often suffer malicious attacks, which may result in network failures. Therefore, how to design more robust defense measures to minimize the loss is a great challenge. In recent years, defense strategies for enhancing the robustness of the networks are developed based on the game theory. However, the aforementioned method cannot effectively solve the defending problem on large-scale networks with a full strategy space. In this study, we achieve the purpose of protecting the infrastructure networks by allocating limited resources to monitor the targets. Based on the existing two-person zero-sum game model and the Double Oracle framework, we propose the EMSL algorithm which is an approximation algorithm based on a greedy search to compute effective mixed strategies for protecting large-scale networks. The improvement of our approximation algorithm to other algorithms is discussed. Experimental results show that our approximation algorithm can efficiently compute the mixed strategies on actual large-scale networks with a full strategy space, and the mixed defense strategies bring the highest utility to a defender on different networks when dealing with different attacks.

Keywords: network robustness, complex network, game theory, mixed strategies, defense

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Jiuchuan Jiang,
Nanjing University of Finance and Economics, China
Zhihai 'Rong,
University of Electronic Science and Technology of China, China

****Correspondence:***
Hong Ding
dinghong@hdu.edu.cn

Specialty section:
This article was submitted to Social Physics,
a section of the journal
Frontiers in Physics

Received: *30 October 2021*
Accepted: *24 November 2021*
Published: *21 December 2021*

Citation:
Wang Z, Jiang M, Yang Y, Chen L and Ding H (2021) Computing Effective Mixed Strategies for Protecting Targets in Large-Scale Critical Infrastructure Networks.
Front. Phys. 9:805584.
doi: 10.3389/fphy.2021.805584

1 INTRODUCTION

In recent years, malicious activities against the critical infrastructures lead to new challenges to the world's security, which have inflicted enormous economic losses and threatened public safety. For instance, in July 2019, a cyber attack on a Venezuelan hydroelectric power plant collapsed the water grid in the capital and more than 10 states, plunging the entire country into darkness [1]. Very recently, the largest oil pipeline company in the United States, Colonial Pipeline, was attacked by the hacker organization DarkSide, which led the country to announce an emergency state [2]. Thus, analyzing the robustness of the critical infrastructure networks against the malicious attacks and accordingly improving the efficiency of defending the targets with limited resources remain major problems.

Prior works have designed methods to protect the critical infrastructure networks against malicious attacks, and we summarize them into three classes. The first class comes up with adding nodes (e.g., adding additional base stations), adding edges (e.g., adding additional power lines), or swapping edges (e.g., rewiring power lines) to enhance the network robustness [3–5]. But these methods will change the network structure, while the structure of a network is a defining characteristic that can identify its functionality and thus should remain unchanged. The second class proposes resource-allocation methods to significantly reduce the time cost of allocating resources and increase the probability of successful defending tasks, considering the cooperativity between resources and tasks [6, 7], which will increase the complexity of the defending problem. The third class develops algorithms to monitor (e.g., closely monitor substation) or immunize important nodes for protecting networks, according to a range of network centrality measures (e.g., degree centrality and betweenness centrality) [8–13]. However, all these existing centrality metrics do not consider the protector's combinatorial pure policy space. Though these defending policies can protect the network against attacks to a certain extent, we can consider mixing the pure strategies and scheduling the defense resources dynamically to design more protective defending strategies.

To address the problem of designing more robust measures for defending the critical infrastructure networks, we can model the urban infrastructure cybersecurity problem as a problem with both defender and attacker participants. The infrastructure-based confrontation between the attacker and the defender can be modeled using game theory. However, most of the research studies that compute the attack and defense strategies by establishing different game models only consider a few typical strategies to shrink the space of strategies, rather taking a large strategy set into account [14–19]. Only one article is distinct; Li et al. proposed the two-player zero-sum simultaneous-move game model to solve the defending problem [20]. Their algorithm enumerates all strategies for obtaining the Nash equilibrium (ESE) on the network with 20 nodes and computes mixed strategies for both players. Unfortunately, their algorithm cannot solve the problem of computing the global equilibrium in large-scale networks. So, the challenge is how to compute effective strategies with the full strategy space of both players growing exponentially with the increase of the network size.

To solve the pervious challenge, based on the existing two-person zero-sum model and settings, we propose our solution containing four key contributions:

1) First, we extend the defending problem to a real large-scale infrastructure network that is vulnerable.
2) Second, we propose the effective mixed strategies for large-scale networks (EMSL) algorithm, which is based on greed under the Double Oracle framework to obtain an effective defense solution.
3) Third, we design mixed-integer linear programming (MILP) to compute the best pure attack strategy for an attacker.
4) Finally, we conduct extensive experiments on two networks of different sizes by comparing with other defense strategies under different attacks. The experimental results show that the mixed defense strategies obtained by our approximation algorithm bring the highest utility to a defender on different networks when dealing with different attacks.

2 INFRASTRUCTURE NETWORK PROTECTING GAME

As in the pioneering work [14], we define the problem of protecting targets in infrastructure networks as a single-round defender–attacker zero-sum game. The defender chooses a subset of nodes to protect, while the attacker chooses some nodes to attack in the target network. Only the nodes chosen by the attacker, meanwhile not protected by the defender, will be removed from the network, and then the payoff function for both players is determined by the remaining network. Both players are assumed to have the complete information of the target network and full knowledge about the opponent. Hence, they are fully aware of all the strategies that the opponent may adopt, as well as the payoffs to each other under each combination of strategies. Nevertheless, the game is a simultaneous one, that is to say, the players do not know exactly which nodes the opponent will choose when making their own decisions.

2.1 Network

The infrastructure system can be easily abstracted as a target network, which is formalized in terms of a simple undirected graph $G = (V, E)$. Each node $v \in V$ represents an infrastructure, where V is the set of nodes in the network. An edge $e_{ij} = (v_i, v_j) \in E$ denotes a directionless edge with v_i and v_j as endpoints, while $E \subseteq V \times V$ denotes the set of edges. We define $N = |V|$ as the number of nodes in the network.

The connectivity between nodes is the equivalence relation on the node $v \in V$. Based on the equivalence relation, V can be divided into several non-empty subsets $V_1, V_2, \ldots, V_n$, and each non-empty subset V_i determines a connected subgraph $G(V_i)$. Especially for a node $v \in V$, we denote the node's connected neighbors as follows:

$$V' = \{u \in V \ \backslash \{v\} | (u, v) \in E, distance\,(u, v) \neq \infty, v \in V\}, \quad (1)$$

where $distance(u, v) \neq \infty$ indicates that there always exists a path from u to v. The connected subgraph $(V', E \cap \binom{V'}{2})$ induced by V' is denoted by $G(V')$. So, $G(V_1), G(V_2), \ldots, G(V_n)$ are defined as the connected components of G. Let $G(V_{max})$ represent the largest connected component (LCC) of G, where V_{max} is defined as the largest connected node subset of V.

Let $\tilde{V} \subseteq V$ denote the subset of nodes in V and $\tilde{E} \subseteq E$ denote the set of edges where each edge in $\tilde{E}$ is connected to at least one node in $\tilde{V}$. The graph $\hat{G} = (\hat{V}, \hat{E})$ obtained by removing all nodes in $\tilde{V}$ and all associated edges in $\tilde{E}$ from G is expressed as follows:

$$\hat{G} = G - \tilde{V}. \quad (2)$$

2.2 Strategies

A pure defender strategy $D = \langle d_v \rangle$ is an assignment of the R_D defending resources to R_D vertices, that is, $\sum_{v \in V} d_v = R_D$, where $d_v \in \{0, 1\}$. $d_v = 1$ indicates the node v is protected by a defender and will never be deleted. We define the set of nodes protected by the defender as $V^D = \{v \in V | d_v = 1\}$, where $|V^D| = R_D$. The defender's strategy space is defined as $\mathbb{D}$. So, a mixed attacker strategy $\mathbf{x} = \langle x_D \rangle$ is a probability distribution over pure strategies, with x_D representing the probability that the pure strategy D is played.

Meanwhile, the attacker can choose a subset of nodes $V^A \subseteq V$ to plan an attack. A pure attacker strategy is defined as a vector $A = \langle a_v \rangle \in \mathbb{A}$, where $\mathbb{A}$ represents the attacker's strategy space and $\sum_{v \in V} a_v = R_A$ indicates that the attacker's resource number is R_A. If $v \in V^A$, then $a_v = 1$; otherwise, $a_v = 0$. A mixed attacker strategy $\mathbf{y} = \langle y_A \rangle$ is a probability distribution over pure strategies, with y_A representing the probability that the pure strategy A is played.

2.3 Utility

In our defender–attacker zero-sum game, given a defender's strategy D and an attacker's strategy A, only when $a_v = 1$, and $d_v = 0$, the node v will be deleted from the network by the attacker; otherwise, the defender protects the targets successfully. If the attacker succeeds, he will receive a payoff P_A and the defender's payoff P_D will be $-P_A$; otherwise, both players will gain 0.

In many critical infrastructure systems, the targets are networked and the functionality relies heavily on the connectivity and topology structures. If the network connectivity decreases during the node deletion, the performance of the networks will degrade. The node number of the largest connected component (N_{LCC}) of the graphs is a robust measure function which is widely used to evaluate the network performance. Hence, we adopt N_{LCC} to construct the payoff functions. $N_{LCC}(G)$ is calculated by determining the maximal connected node subset $V_{max} \subseteq V$ in G [21], and it can be expressed as follows:

$$N_{LCC}(G) = |V_{max}|. \tag{3}$$

If the defender's strategy D and the attacker's strategy A select sets of nodes differently, that is, $V^A \cap V^D \neq V^D$, which means the defender fails in protecting the targets and the attacker succeeds, then the node subset $\tilde{V} = V^A - V^A \cap V^D$ and its associated edge set $\tilde{E}$ will be deleted from the target network, and we define $\hat{V}_{max} \subseteq (V - \tilde{V})$ as the largest connected node subset of the residual graph $\hat{G}$. $N_{LCC}(\hat{G})$ is computed by determining the size of $\hat{V}_{max}$ as follows:

$$N_{LCC}(\hat{G}) = |\hat{V}_{max}|, \tag{4}$$

where $\hat{V}_{max} \subseteq (V - (V^A - V^A \cap V^D))$ in $\hat{G}$. Otherwise, if the defender protects the network successfully, that is, $V^A \cap V^D = V^D = V^A$, which means that no node will be deleted from G, then $N_{LCC}(\hat{G}) = N_{LCC}(G)$.

Hence, the payoff function of the attacker P_A is defined as follows:

$$P_A = \frac{N_{LCC}(G) - N_{LCC}(\hat{G})}{N_{LCC}(G)} \in [0, 1] \tag{5}$$

and the defender's payoff function P_D is given as follows:

$$P_D = \frac{N_{LCC}(\hat{G}) - N_{LCC}(G)}{N_{LCC}(G)} \in [-1, 0], \tag{6}$$

where N_{LCC} can be replaced by any other measure functions that meet the monotonicity assumption.

After the payoff functions of the players are obtained, we define U_D as the expected utility function of the defender. Given a defender's mixed strategy $\mathbf{x}$ and an attacker's pure strategy A, the expected defender utility $U_D(\mathbf{x}, A)$ is given as follows:

$$U_D(\mathbf{x}, A) = \sum_{D \in \mathbb{D}} (1 - z_{D,A}) x_D P_D, \tag{7}$$

where $z_{D,A}$ indicates whether the defender strategy D successfully protects the targets that are attacked by A, that is, $z_{D,A} = 0$ if $D \cap A = D$ or 1 otherwise.

The defender's expected utility $U_D(D, \mathbf{y})$ of playing a pure defense strategy D against the mixed attack strategy $\mathbf{y}$ is

$$U_D(D, \mathbf{y}) = P_D \sum_{A \in \mathbb{A}} (1 - z_{D,A}) y_A. \tag{8}$$

When playing a mixed defense strategy $\mathbf{x}$ against the mixed attack strategy $\mathbf{y}$, the defender's expected utility $U_D(\mathbf{x}, \mathbf{y})$ is given as follows:

$$U_D(\mathbf{x}, \mathbf{y}) = \sum_{D \in \mathbb{D}} x_D U_D(D, \mathbf{y}) = \sum_{A \in \mathbb{A}} y_A U_D(\mathbf{x}, A). \tag{9}$$

Generally, based on the two-person zero-sum game, we note $U_A = -U_D$.

2.4 Equilibrium

The Nash equilibrium of two-person zero-sum games is the maximum equilibrium. The aim of the defender is to protect the target nodes of the network to maximize their minimum utility and minimize the attacker's maximum utility. We use linear programming to solve the zero-sum game. The defender's optimal mixed strategy $\mathbf{x}$ can be computed by solving the following linear programming (LP):

$$\max \quad U \tag{10}$$

$$s.t. \quad U \leq U_D(\mathbf{x}, A), \forall A \in \mathbb{A}, \tag{11}$$

$$\sum_{i=1}^{N} d_v = R_D, \tag{12}$$

$$\sum_{D \in \mathbb{D}} x_D = 1, \tag{13}$$

$$x_D \geq 0, \forall D \in \mathbb{D}. \tag{14}$$

When the strategy spaces of both sides are small, the optimal solution can be obtained by solving the programming **Equations 10–14**. However, as the network scale expands, the defender's strategy space $\mathbb{D}$ and the attacker's strategy space $\mathbb{A}$ will grow exponentially with the number of resources R_D. At this time, it is difficult to calculate the optimal solution in a short time by mathematical programming, so it is necessary to design new algorithms to get efficient strategies for both players.

3 APPROACH

In this section, we first give a brief introduction to the ESE algorithm, which is very similar to the problem solved in this study [20], and analyze the limitations of the algorithm. Then we propose our EMSL algorithm and describe it in detail.

3.1 Limitation of ESE Algorithm

The ESE algorithm is adopted by Li et al., which solves the attacker–defender game by computing the global equilibrium with full strategy space on a small network [20]. First, they enumerate all possible attack and defense strategies and calculate the payoffs of the players in each strategy to construct the payoff matrix. Next, they start the two-person zero-sum game by choosing nodes with the largest degrees to attack, satisfying the resource constraint, and identify the defender's best response to the attacker's strategy. Then they compute the best response pure strategies over the payoff matrix for the players. Finally, the Nash equilibrium is computed to calculate the players' best mixed response strategies over each pure strategy.

Unfortunately, the ESE algorithm can only be solved on the network with 20 nodes. Since the strategy space is too large as the network scale grows, it is very time-consuming to calculate the payoffs in each strategy profile one by one. It is impossible to solve the problem by enumerating all strategies to maximize the benefits of both the attacker and the defender. So, the ESE algorithm cannot be applied to real large-scale networks due to its limited computing power.

We find that the interaction process of the players in the ESE algorithm is similar to the Double Oracle (DO) framework. The DO framework is a standard method for solving zero-sum games with large strategy spaces.

However, there are two challenges to solving the INP game under the DO framework: 1) We can only present the MILP for computing the best response strategy of the attacker (in **Section 4.2**), and we solve it on the network with 20 nodes. The best attack method is used as an attack method for comparison in the experiments. But it is difficult to present the MILP for computing the best response strategy of the defender because of the weakness of high complexity. 2) Computing the MILP is time-consuming, and it is difficult to solve it for an optimal solution on large networks. We aim to find an efficient solution for the INP problem, but not an optimal solution. The effective solution can be obtained by designing an approximate algorithm under the suboracles of DO framework. Hence, we propose the effective mixed strategies for large-scale networks (EMSL) algorithm for computing the improved solution.

3.2 EMSL Algorithm

To solve the INP problem, we propose our EMSL algorithm based on greedy search under the DO framework. The DO framework can efficiently solve the zero-sum games on real large networks. For instance, Jain et al. proposed the SNARES algorithm to solve the security scheduling problem on the Mumbai road network with 9,503 nodes and 20,416 edges [22]. And Wang et al. introduced the DO-TPD algorithm to compute an optimal monitoring strategy for detecting terrorist plots on realistic-sized problems, which contains about 100 such potential terrorists in some 1,400 French nationals [23]. The DO framework is formed from Defender Oracle and Attacker Oracle. And both of the oracles contain Best Oracle and Better Oracle. Best Oracle can compute the optimal solution by solving the MILP, instead of enumerating all possible strategies, while Better Oracle can improve the computing efficiency for an approximate solution. Due to the challenges of solving Best Oracle mentioned in **Section 3.1**, we design the EMSL algorithm under Better Oracle (EMSL-Better-O). It is sketched in Algorithm 1.

Algorithm 1. EMSL-Better-O overview (G, R_D, R_A).

```
   Input: $G = \langle V, E \rangle$, $R_D$, $R_A$
   Output: Mixed strategies $(\mathbf{x}, \mathbf{y})$
1  Initialize $\mathbb{D}'$, $\mathbb{A}'$ randomly ;
2  repeat
3      $(\mathbf{x}, \mathbf{y}) \leftarrow CoreLP(\mathbb{D}', \mathbb{A}')$;
4      $\mathbb{D}^{+} \leftarrow betterO - D(\mathbf{x}, \mathbf{y})$;
5      $\mathbb{D}' \leftarrow \mathbb{D}' \cup \mathbb{D}^{+}$;   /*Lines 4-5: Defender Oracle */
6      $\mathbb{A}^{+} \leftarrow betterO - A(\mathbf{x}, \mathbf{y})$;
7      $\mathbb{A}' \leftarrow \mathbb{A}' \cup \mathbb{A}^{+}$;   /*Lines 6-7: Attacker Oracle */
8  until $\mathbb{D}^{+} = \emptyset$ and $\mathbb{A}^{+} = \emptyset$;
```

Line 1 first initializes EMSL-Better-O by generating a small strategy space $\langle \mathbb{D}', \mathbb{A}' \rangle$ randomly. Then **Equation 9** computes the equilibrium with $\langle \mathbb{D}, \mathbb{A} \rangle$ replaced by $\langle \mathbb{D}', \mathbb{A}' \rangle$ to solve the restricted version of INP (CoreLP, Line 3). The restricted INP can be solved efficiently because the strategy space $\langle \mathbb{D}', \mathbb{A}' \rangle$ is small. Obviously, the solution obtained is an equilibrium of the restricted INP and does not form an equilibrium to the original INP. So, both players want to improve their utilities with other strategies out of $\langle \mathbb{D}', \mathbb{A}' \rangle$. EMSL-Better-O allows them to do so with Better Oracle (Lines 4–5 and Lines 6–7). Specifically, EMSL-Better-O calls BetterO-D (Better Oracle for Defender) to search a set of improving strategies for the defender (Lines 4–5). And in the similar manner, EMSL-Better-O calls BetterO-A (Better Oracle for Attacker) to find improving strategies for the attacker (Lines 6–7). The process repeats until no improving strategy can be found for both players (Line 8), when the final solution obtained for the original INP is close to optimal.

The EMSL-Better-O algorithm of Defender Oracle (EMSL-Better-OD) is presented in Algorithm 2. EMSL-Better-OD generates a defender pure strategy D_{Better}. The core of each iteration (Lines 5–8) is designed based on the greedy search.

Algorithm 2. EMSL-Better-OD (**x**, **y**).

```
    Input: $(\mathbf{x}, \mathbf{y})$
    Output: $\mathbb{D}_{Better}$
1   Initialize $D_{Better} = \emptyset$;
2   Start with $D$ randomly, $A \leftarrow \mathbf{y}$;
3   repeat
4       for $v \in V$ do
5           while no termination condition is met do
6               $D' \leftarrow GreedySearch(v, D, \mathbf{y})$;
7               if $U_D(D', \mathbf{y}) > U_D(D, \mathbf{y})$ then
8                   $D \leftarrow D'$;
9           if $U_D(D, \mathbf{y}) > U_D(\mathbf{x}, \mathbf{y})$ then
10              $\mathbb{D}_{Better} \leftarrow \mathbb{D}_{Better} \cup D$;
11  until $U_D(\mathbb{D}_{Better}, \mathbf{y}) = U_D(\mathbf{x}, \mathbf{y})$;
```

EMSL-Better-OD repeatedly starts from an empty strategy space $\mathbb{D}_{Better}$ and initializes a random pure strategy $D \in \mathbb{D}$ (Lines 1–2). Then in a greedy manner, it iteratively applies $GreedySearch(v, D, \mathbf{x})$ (Algorithm 3) for a new local optimal strategy D' that brings the maximum utility to the defender (Line

6). Afterward, the strategy set D is updated systematically by D' (Lines 7–8). The loop repeats until the termination conditions are met: 1) $U_D(D, \mathbf{y}) > U_D(\mathbf{x}, \mathbf{y})$; 2) $D^+ = \varnothing$; and 3) $U_D(D, \mathbf{y}) - U_D(\mathbf{x}, \mathbf{y}) < \epsilon$, where ϵ is a pre-defined global variable to constrain the total number of iterations. The defense strategy $\mathbb{D}_{Better}$ is computed over the local optimal strategies (Lines 9–10). Compared with enumerating all strategies to construct a payoff matrix and calculating the global equilibrium, our algorithm based on greedy search effectively improves the computing power.

Algorithm 3. *GreedySearch*(v, D, $\mathbf{x}$).

```
   Input: $(\mathbf{x}, \mathbf{y})$
   Output: A pure defense strategy $D$
 1 Start with $D = \emptyset$;
 2 repeat
 3     for $v \in V$ do
 4         $v' \leftarrow argmax_{v \in V^D} U_D(D \cup \{v\}, \mathbf{y})$;
 5         if $U_D(D \cup \{v'\}, \mathbf{y}) > U_D(D, \mathbf{y})$ then
 6             $D \leftarrow D \cup \{v'\}$;
 7         else
 8             $v' \leftarrow argmax_{v \in D \setminus (V^D \cup \{v\})} U_D(D \setminus \{v\}, \mathbf{y})$;
 9             if $U_D(D \setminus \{v'\}, \mathbf{y}) > U_D(D, \mathbf{y})$ then
10                 $D \leftarrow D \setminus \{v'\}$;
11 until $|D| = R_D$;
```

The goal of *GreedySearch* (v, D, $\mathbf{x}$) is to find a pure defense strategy that can improve the defender's utility. It repeatedly starts from an empty strategy $D = \varnothing$, and it consecutively tries to add a best node v' in the hope of improving the defender's utility U_D (Line 4). If the node v' satisfies $U_D(D \cup \{v'\}, \mathbf{y}) > U_D(D, \mathbf{y})$, then $D \leftarrow D \cup \{v'\}$ (Lines 5–6); otherwise, it tries to add a best node v' from the rest node set $D \backslash \{v'\}$ (Line 8). If $U_D(D \backslash \{v'\}, \mathbf{y}) > U_D(D, \mathbf{y})$, then $D \leftarrow D \backslash \{v'\}$ (Line 9–10). Finally, it stops when $|D| = R_D$. Note that the utility function is a submodular set function, which guarantees the approximate solution a $(1 - \frac{1}{e})$ approximation ratio to the optimal solution [24].

The time complexity of our approximate algorithm is $O(N^2)$, and the spatial complexity is $S(N^2)$, where N is the size of the networks. Our algorithm can be solved within a limited time complexity.

4 EXPERIMENTAL RESULTS AND ANALYSIS

We assess the performance of our approach through a number of experiments. The algorithms proposed in this article are coded in Visual Studio. Core-LP and MILP are solved by calling CPLEX. All computations are performed on a machine with a 3.60 GHz quad core CPU and 8.00 GB memory. The parameter ϵ in EMSL-Better-OD (Algorithm 2) is set to be 0.05. The number of defense resources R_D is set to be $\frac{1}{5} * N$ (see **Section 4.3.1**), and the attack resource number R_A is set to be equal and variable from 0 to N. We conduct experiments on two types of graphs with $N_1 = 20$ and $N_2 = 500$.

In this section, the defense methods for comparison and the attack methods for confrontation are introduced first. Then the solution of the approximate algorithm on two different networks is presented and analyzed.

4.1 Defense Methods for Comparison

It is essential to prove the effect of the defender's mixed strategies with other defense methods. The typical defense methods we used for comparison are as follows:

1) ID Defense [25]: In the initial network, the degree of each node is first calculated in the network, and then the vertex is chosen in descending order from the highest vertex to defense. After each attack, the network structure will change, and the degree of each node may also change, but it will not be recalculated. That is to say, the defending strategy uses the initial degree distribution, so we call it the "ID Defense" method.
2) IB Defense [25]: In the initial network, the betweenness of each node is calculated first, and then the vertex is selected for defense according to the descending order of betweenness. Similarly, this defending strategy is also distributed according to the initial mediation degree, so it is called the "IB Defense" method.
3) RA Defense: In the initial network, nodes are randomly selected for defense. In this article, we call it the "RA Defense" method. It should be noted that although random selection seems to be the most convenient way, some key nodes may be selected, which makes the experimental results accidental. In order to avoid the occurrence of the previous situation, we will repeat the process of selecting nodes randomly and calculating the results when carrying out RA Defense. Finally, the average of all the results is calculated as the final result.
4) DCM Defense [26]: In the initial network, nodes are defended by the mixed strategies, where the marginal coverage probability of each vertex is normalized degree centrality. Given the marginal coverage probabilities, the mixed strategies are generated using the comb sampling algorithm.

4.2 Attack Methods

Considering the actual situation that attackers may take many kinds of attacks to achieve their goals, it is also important to verify that the defender's mixed strategy obtained by the approximate algorithm is efficient due to different attacks. Many relative works analyze the robustness of the critical infrastructure networks against malicious attacks. The first class estimates the robustness by removing nodes or edges based on the load capacity [27–30]. The second class comes up with removing some nodes or edges based on the degree distribution or betweenness distribution of the networks [10, 28, 29, 25, 13, 31, 32]. The third class develops the method of the tabu search into the network disintegration problem to identify the optimal attack strategy is introduced [33].

So, based on the model and scenario of this study, the attack methods we chose for confrontation are as follows:

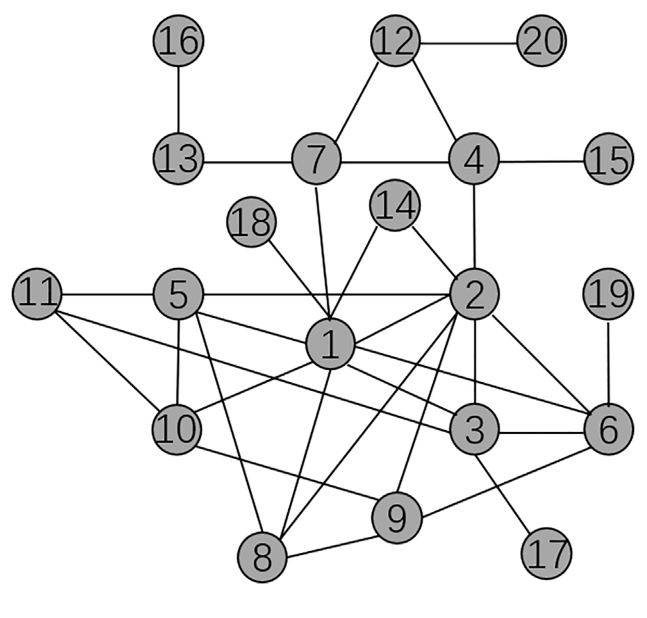

FIGURE 1 | Topology structure of a small network with 20 nodes [20].

1) ID Attack: Attacking nodes based on the initial degree distribution of the network.
2) IB Attack: Attacking nodes based on the initial betweenness distribution of the network.
3) RA Attack: Attacking nodes randomly in the networks.
4) BEST-OA Attack: Attacking nodes with the best attack strategy. We consider the worst case, that is, assuming that the attacker always chooses the most destructive attack method. So, we use mixed-integer linear programming (MILP) to solve the best pure attack strategy for an attacker, and it is called the "BEST-OA Attack" method. The MILP is shown in the following equations:

$$\max \quad \sum_{D\in\mathbb{D}} \left(\frac{N_{LCC}(G)-N_{LCC}(\hat{G})}{N_{LCC}(G)}\right)\cdot x_D \tag{15}$$

$$s.t. \quad \sum_{D\in\mathbb{D}} x_D = 1, x_D \geq 0, \forall D \in \mathbb{D}, \tag{16}$$

$$\sum_{i=1}^{N} a_v = R_A, a_v \in V^A, a_v \in \{0,1\}, \tag{17}$$

$$\sum_{i=1}^{N} d_v = R_D, d_v \in V^D, d_v \in \{0,1\}, \tag{18}$$

$$d_v \cdot a_v - d_v < v_i^{DA} < d_v \cdot a_v - d_v + 2, \tag{19}$$

$$v_i^{DA} + v_j^{DA} - 1 \leq e_{ij}^{DA}, v_i^{DA} \in \{0,1\}, e_{ij}^{DA} \in \{0,1\}, \tag{20}$$

$$e_{ij}^{DA} \leq v_i^{DA}, e_{ij}^{DA} \leq v_j^{DA}, \tag{21}$$

$$\sigma_{jk}^{DA} - \sigma_{ik}^{DA} \geq e_{ij}^{DA} - 1, \sigma_{ij}^{DA} \in \{0,1\}, \tag{22}$$

$$N_{LCC}(\hat{G}) \geq \sum_{v_i \in V^D} \sigma_{ij}^{DA}, \tag{23}$$

where $v_i^{DA} = 1$ represents the node v_i is still in $\hat{G}$ when it is attacked by A under the protection of D; otherwise, $v_i^{DA} = 0$. $e_{ij}^{DA} = 1$ represents the edge between nodes v_i and v_j is still in $\hat{G}$ when it is attacked by A under the protection of D; otherwise, $e_{ij}^{DA} = 0$. $\sigma_{ij}^{DA} = 1$ represents nodes v_i and v_j are still in the same connected subgraph when they are attacked by A under the protection of D; otherwise, $\sigma_{ij}^{DA} = 0$. Specifically, $\sigma_{ii} = 1$. **Equations 19–23** constrain the existence of connected subgraphs after attack. The goal of defenders in best attack oracle is to verify an optimal attack strategy over the entire pure strategy space. Unfortunately, solving best attack oracle turns out to be NP-hard, and the MILP only can be solved on small networks [23].

4.3 Solution of the Approximation Algorithm

To verify the performance of the mixed defense strategies, we solve the defender–attacker model by conducting experiments on a small network with 20 nodes first, which is used by Li [20], and then extend to the U.S. air transportation network with 500 nodes [34]. At the same time, the evolution of robustness of networks is analyzed under two topological changes.

4.3.1 Effectiveness of the Mixed Defense Strategies on Small Network

A small network topology structure with 20 nodes is shown in **Figure 1**. The numbers of attack resources R_A and defense resources R_D are set to be equal and variable from 0 to 20. To validate the effectiveness of the mixed strategy in small networks, we compare the results with those of some other typical defense strategies under different attack methods. The typical defense strategies for comparison here are ID Defense, IB Defense, RA Defense, DCM Defense, and NO Defense which means $R_D = 0$. The curve of NO Defense is shown as a baseline. And the attack strategies used in this section are ID Attack, IB Attack, RA Attack, and BEST-OA Attack. These comparison defense strategies and attack strategies have been introduced in the previous subsections.

• Effectiveness Analysis

As shown in **Figures 2A–D**, what the curves represent are the defender's utility, while $R_D = 4$ and R_A is variable from 0 to 20 on a small network. The vertical axis represents the defender's utility, and the horizontal axis represents the number of attack resources. A higher defender utility indicates a lower attacker utility given the zero-sum assumption as well as better performance of the mixed defense strategy. The results show that with the increase of attack resources, the decline rate of defender's utility is the slowest under the protection of the mixed defense strategy. And no matter in which attack mode, the defender's utility obtained by the mixed defense strategy is higher than that obtained by other defense methods, especially in the case of RA Attack. Although under IB Attack, the results of IB defense, RA Defense, and mixed strategy defense are close to each other, the mixed strategy is still performing the best (**Figure 2B**). The results are sufficient enough to indicate the effectiveness of our approximation algorithm in small networks.

- Optimal defense resource number based on unit resource efficiency

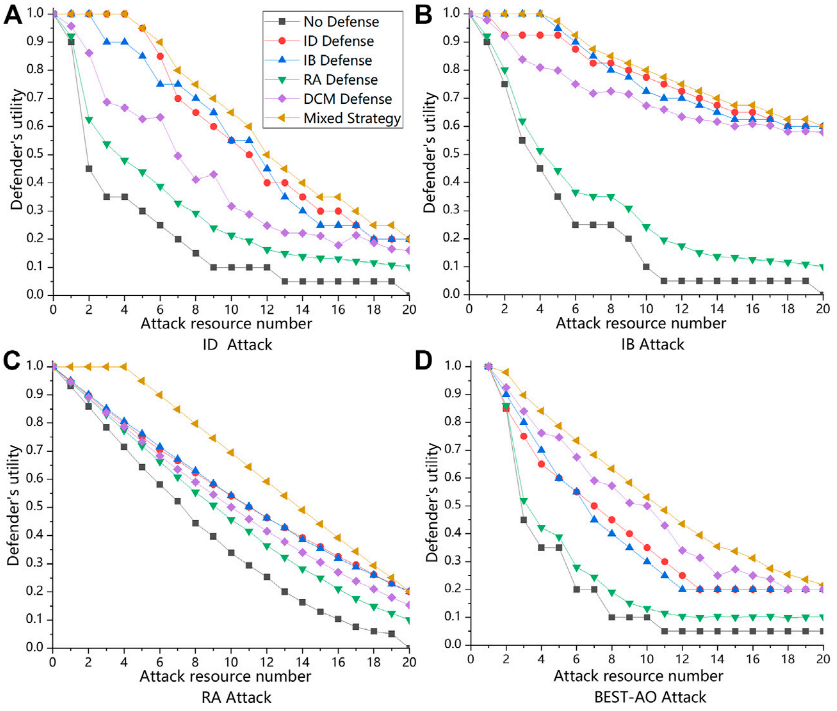

FIGURE 2 | These are defender's utility of the mixed defense strategy and other comparison defense methods under different attack methods while $R_A = 4$ on small network with $|V| = 20$. R_D is variable from 0 to 20. **(A)** is the defender's utility when playing ID Attack strategy with different defense strategies. **(B)** is the defender's utility when playing IB Attack strategy with different defense strategies. **(C)** is the defender's utility when playing RA Attack strategy with different defense strategies. **(D)** is the defender's utility when playing BEST-AO Attack strategy with different defense strategies.

TABLE 1 | Utility of the defender when the BEST-OA Attack method confronts the ID Defense method.

$R_A \vert R_D$	0	1	2	3	4	5	6	7	8	9	10
0	1	1	1	1	1	1	1	1	1	1	1
1	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.9	0.9	0.9	0.9
2	0.45	0.65	0.65	0.65	0.75	0.75	0.75	0.8	0.8	0.8	0.8
3	0.35	0.55	0.55	0.55	0.65	0.65	0.7	0.75	0.75	0.75	0.75
4	0.35	0.45	0.45	0.5	0.6	0.6	0.65	0.7	0.7	0.7	0.7
5	0.2	0.4	0.4	0.45	0.55	0.55	0.6	0.65	0.65	0.65	0.65
6	0.2	0.3	0.3	0.4	0.5	0.5	0.55	0.6	0.6	0.6	0.6
7	0.1	0.25	0.25	0.35	0.45	0.45	0.5	0.55	0.55	0.55	0.55
8	0.1	0.15	0.2	0.3	0.4	0.4	0.45	0.5	0.5	0.5	0.5
9	0.1	0.1	0.15	0.25	0.35	0.35	0.4	0.45	0.45	0.45	0.5
10	0.05	0.1	0.1	0.2	0.3	0.3	0.35	0.4	0.4	0.45	0.5

TABLE 2 | Increment of the defender's utility.

$R_A \vert R_D$	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0.05	0	0	0
3	0.2	0	0	0.1	0	0	0.05	0	0	0
4	0.2	0	0	0.1	0	0.05	0.05	0	0	0
5	0.1	0	0.05	0.1	0	0.05	0.05	0	0	0
6	0.2	0	0.05	0.1	0	0.05	0.05	0	0	0
7	0.1	0	0.1	0.1	0	0.05	0.05	0	0	0
8	0.15	0	0.1	0.1	0	0.05	0.05	0	0	0
9	0.05	0.05	0.1	0.1	0	0.05	0.05	0	0	0
10	0	0.05	0.1	0.1	0	0.05	0.05	0	0	0.05

With the network growing, it is essential to define the optimal defense resource number R_D. We define the number of resources per unit as 1 resource, adding one unit of resources per experiment. Then we repeatedly calculate the increment of the defender's profit after adding the unit resource under different defense and attack methods. Finally, we calculate the defender's average profit increment. The number of defense resources that maximize the defender's average profit increment is defined as the optimal defense resources.

For example, **Table 1** shows the benefits of the defender when the BEST-OA Attack method confronts the ID Defense method,

TABLE 3 | Average value of the defender's utility increment.

R_D	1	2	3	4	5	6	7	8	9	10
Average	0.0548	0.0262	0.0524	0.0690	0.0214	0.0429	0.0476	0.0238	0.0262	0.0286

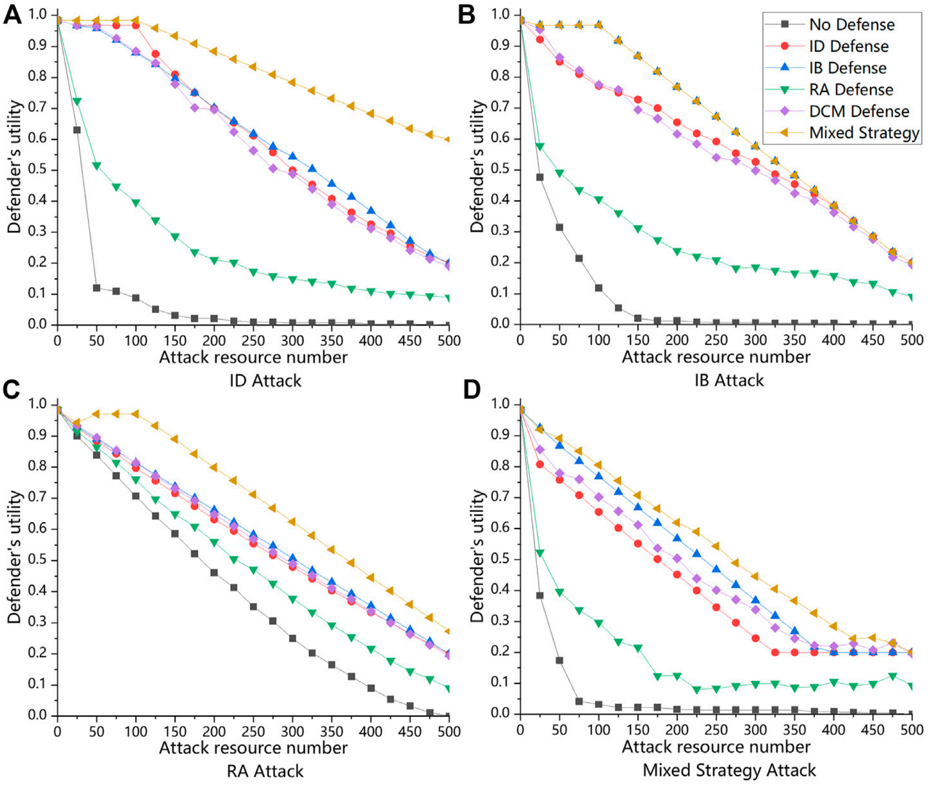

FIGURE 3 | These are defender's utility of the mixed defense strategy and other comparison defense methods under different attack methods while R_D = 100 on the air transportation network with $|V|$ = 500. R_A is variable from 0 to 500. **(A)** is the defender's utility when playing ID Attack strategy with different defense strategies. **(B)** is the defender's utility when playing IB Attack strategy with different defense strategies. **(C)** is the defender's utility when playing RA Attack strategy with different defense strategies. **(D)** is the defender's utility when playing Mixed Attack strategy with different defense strategies.

while R_A and R_D are from 1 to 10. **Table 2** shows the increment of the defender's profit after each increase of unit resources. And **Table 3** shows the average value of the defender's profit increment. We find that when the number of resources is 4, the average increment of the defender's utility is the biggest. So, the optimal defense resource number is 4, which is equivalent to $\frac{1}{5}$ of the total node number on the network with 20 nodes. Hence, when we expand the experiments to a large network of 500 nodes, the corresponding optimal number of defense resources is 100. It is convenient to find the optimal defense resource number in large networks with the aforementioned method, which also can reflect the significance of the experimental results more clearly and intuitively.

4.3.2 Effectiveness of the Mixed Defense Strategies on Real Large-Scale Network

Then to evaluate the solution quality of the approximate algorithm on large-scale networks, we conduct experiments on the U.S. air transportation network with 500 nodes [34], and the defense resource number is set to be R_D = 100. We separately analyze the results of the mixed defense strategy and the mixed attack strategy to further test the performance of the mixed defense strategy. The experimental results are shown in **Figures 3A–D** and **Figures 4A–F**.

In **Figures 3A–D**, these graphs show the defender's utility when using the mixed defense strategy and other comparison defense methods under different attack methods while R_D = 100 on the real large-scale network. All the steps and comparison defense strategies of the experiments in this subsection are the same as in **Subsection 4.3.1**. The attack methods for confrontation are changed to ID Attack, IB Attack, RA Attack, and mixed strategy attack. Since the best attack strategy computed by MILP can only be solved in small networks due to its limited solving ability, we compute the mixed attack strategy by solving the approximate algorithm. In particular, we find that

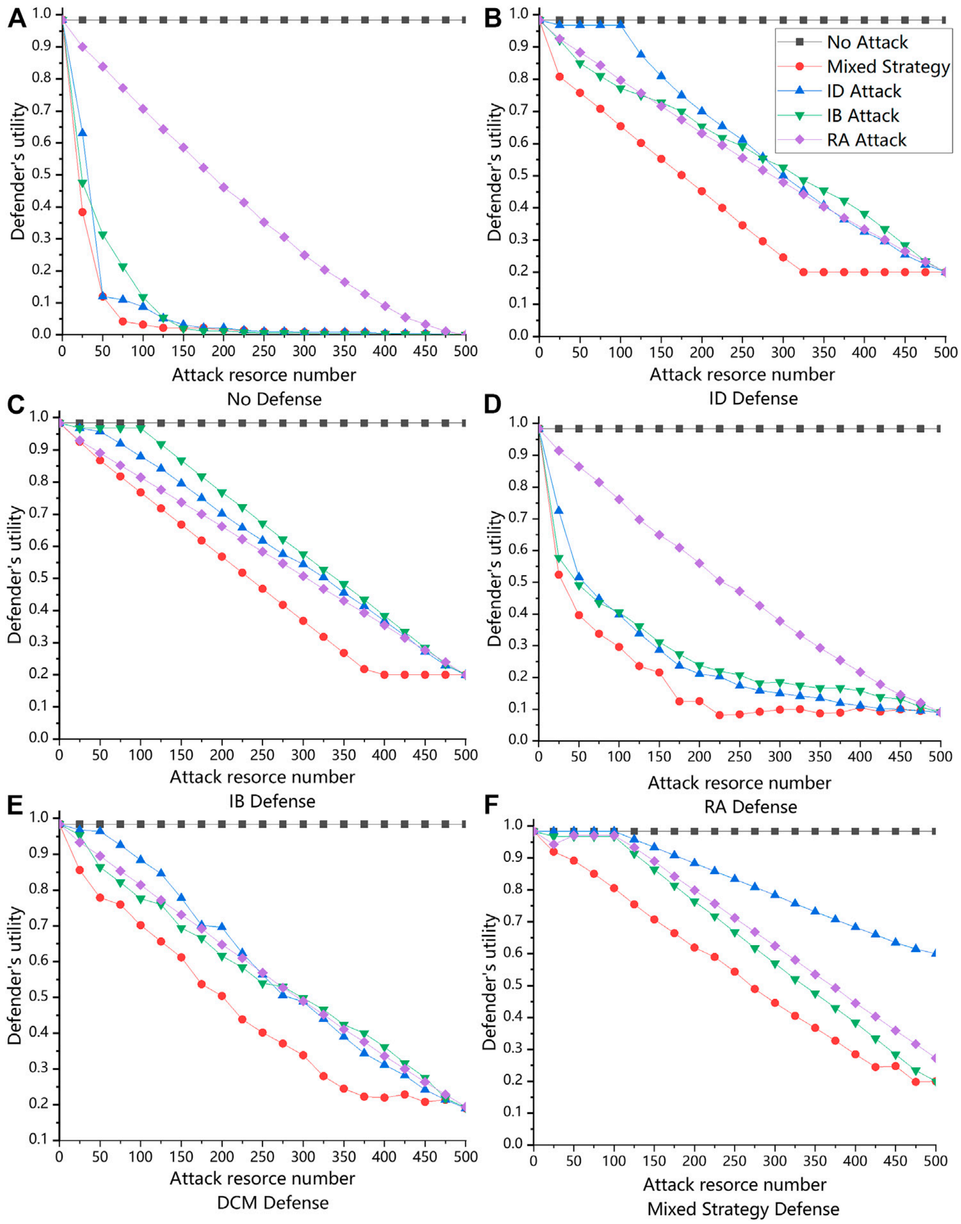

FIGURE 4 | These are defender's utility of the mixed defense strategy and other comparison defense methods under different defense methods while $R_D = 100$ on the air transportation network with $|V| = 500$. R_A is variable from 0 to 500. **(A)** is the defender's utility when playing different attack strategies with no defense. **(B)** is the defender's utility when playing ID Defense strategy with different attack strategies. **(C)** is the defender's utility when playing IB Defense strategy with different attack strategies. **(D)** is the defender's utility when playing RA Defense strategy with different attack strategies. **(E)** is the defender's utility when playing Mixed DCM strategy with different attack strategies. **(F)** is the defender's utility when playing Mixed Defense strategy with different attack strategies.

under IB Attack, the curves of IB Defense and mixed strategy defense are almost coincident (**Figure 3B**), which indicates that IB Defense performs well in dealing with IB Attack and also reflects that our approximation algorithm may fall into local optimization. The final result of our approximate algorithm depends in part on its initial solution. Anyway, in most cases, the results can be better than those of other methods. These figures obviously describe that under the mixed strategy defense, the decline rate of defender's utility is the slowest no matter which attack strategy is used, and the mixed defense strategy can still work well under different attacks in large-scale networks.

Figures 4A–F show the defender's utility when using the mixed attack strategy and other comparison attack methods confronting different defense strategies while $R_D = 100$ on the same real large-scale network. The comparison attack strategies and defense strategies are all the same. The results clearly show that no matter in which attack strategy, the mixed defense strategy always brings the highest utility to the defender and can make the defender's utility decline the slowest in the shortest time. Moreover, it is worth mentioning that the defender's utility obtained by the mixed attack strategy declines the fastest, which also reflects the mixed defense strategy solved by the approximate algorithm can effectively destroy the networks. In summary, these results certainly reflect that the mixed defense strategy performs well in large-scale networks and our approximate algorithm can solve the problem efficiently when scaling up the networks.

5 CONCLUSION

It is a challenge to reasonably design effective defense strategies with limited resources to protect large-scale critical infrastructure networks against malicious attacks. In this study, we first develop an efficient approximation algorithm under the Double Oracle framework to speed up the calculation for computing the mixed defense strategy based on heuristics significantly with given resources. Then we extend the INP problem to a real large-scale infrastructure network to test the performance of the mixed defense strategy. Finally, we conduct extensive experiments on two networks of different sizes by comparing with other defense strategies under various attacks. The experimental results show that our approximation algorithm can ensure a robust enough solution to protect real large-scale networks.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, and further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

ZW contributed to the conception of the study. MJ performed the data analyses and wrote the manuscript. YY performed the experiments. LC and HD helped perform the analysis with constructive discussions.

FUNDING

This research was supported by the Zhejiang Provincial Natural Science Foundation of China (No. LY20F030012) and National Natural Science Foundation of China (62176080).

REFERENCES

1. Jasso C. *"cyberattacks Insider Sabotage": Venezuela's Power Grid Still under Attack – Maduro* (2019). Available at: https://www.rt.com/news/453434-venezuela-maduro-cyberattack-power-grid/ (Accessed October 8, 2021).
2. Wikipedia. *Colonial Pipeline Cyberattack* (2021). Available at: https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack/ (Accessed October 8, 2021).
3. Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ. Mitigation of Malicious Attacks on Networks. *Proc Natl Acad Sci* (2011) 108:3838–41. doi:10.1073/pnas.1009440108
4. Yang Y, Li Z, Chen Y, Zhang X, Wang S. Improving the Robustness of Complex Networks with Preserving Community Structure. *PloS one* (2015) 10:e0116551. doi:10.1371/journal.pone.0116551
5. Liu Y, Wei B, Wang Z, Deng Y. Immunization Strategy Based on the Critical Node in Percolation Transition. *Phys Lett A* (2015) 379:2795–801. doi:10.1016/j.physleta.2015.09.017
6. Jiang Y, Zhou Y, Li Y. Reliable Task Allocation with Load Balancing in Multiplex Networks. *ACM Trans Auton Adapt Syst* (2015) 10:1–32. doi:10.1145/2700327
7. Jiang J, An B, Jiang Y, Zhang C, Cao J. Group-oriented Task Allocation for Crowdsourcing in Social Networks. *IEEE Trans Syst Man, Cybernetics: Syst* (2019) 1–16.
8. Briesemeister L, Lincoln P, Porras P. Epidemic Profiles and Defense of Scale-free Networks. in " Proceedings of the 2003 ACM Workshop on Rapid Malcode, Washington, DC, USA, October 27, 2003 (2003) (New York, NY, USA: Association for Computing Machinery), 67–75. doi:10.1145/948187.948200
9. Beygelzimer A, Grinstein G, Linsker R, Rish I. Improving Network Robustness by Edge Modification. *Physica A: Stat Mech its Appl* (2005) 357:593–612. doi:10.1016/j.physa.2005.03.040
10. Leskovec J, Krause A, Guestrin C, Faloutsos C, VanBriesen J, Glance N. Cost-effective Outbreak Detection in Networks. in " Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, California, USA, August 12–15, 2007 (2007) (New York, NY, United States: Association for Computing Machinery), 420–9. doi:10.1145/1281192.1281239
11. Chen C, Tong H, Prakash BA, Tsourakakis CE, Eliassi-Rad T, Faloutsos C, et al. Node Immunization on Large Graphs: Theory and Algorithms. *IEEE Trans Knowledge Data Eng* (2015) 28:113–26.
12. Tong H, Prakash BA, Tsourakakis C, Eliassi-Rad T, Chau DH. *On the Vulnerability of Large Graphs*. IEEE International Conference on Data Mining (2010).
13. Liu Y, Sanhedrai H, Dong G, Shekhtman LM, Wang F, Buldyrev SV, et al. Efficient Network Immunization under Limited Knowledge. *Natl Sci Rev* (2021) 8:nwaa229. doi:10.1093/nsr/nwaa229
14. Li Y-P, Tan S-Y, Deng Y, Wu J. Attacker-defender Game from a Network Science Perspective. *Chaos* (2018) 28:051102. doi:10.1063/1.5029343
15. Zeng C, Ren B, Li M, Liu H, Chen J. Stackelberg Game under Asymmetric Information in Critical Infrastructure System: From a Complex Network Perspective. *Chaos* (2019) 29:083129. doi:10.1063/1.5100849
16. Li Y, Qiao S, Deng Y, Wu J. Stackelberg Game in Critical Infrastructures from a Network Science Perspective. *Physica A: Stat Mech its Appl* (2019) 521:705–14. doi:10.1016/j.physa.2019.01.119
17. Zeng C, Ren B, Liu H, Chen J. Applying the Bayesian Stackelberg Active Deception Game for Securing Infrastructure Networks. *Entropy* (2019) 21:909. doi:10.3390/e21090909
18. Zhang X, Ding S, Ge B, Xia B, Pedrycz W. Resource Allocation Among Multiple Targets for a Defender-Attacker Game with False Targets Consideration. *Reliability Eng Syst Saf* (2021) 211:107617. doi:10.1016/j.ress.2021.107617
19. Ma L, Liu J, Duan B. Evolution of Network Robustness under Continuous Topological Changes. *Physica A: Stat Mech its Appl* (2016) 451:623–31. doi:10.1016/j.physa.2016.01.088
20. Li Y, 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) 6:56214–21. doi:10.1109/access.2018.2872767
21. Freitas S, Yang D, Kumar S, Tong H, Chau DH. *Graph Vulnerability and Robustness: A Survey*. arXiv preprint arXiv:2105.00419 (2021).
22. Jain M, Conitzer V, Tambe M. "Security Scheduling for Real-World Networks," in Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems, St. Paul, MN, USA, May

6–10, 2013 (2013) (Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems), 215–22. doi:10.5555/2484920

23. Wang Z, Yin Y, An B. “Computing Optimal Monitoring Strategy for Detecting Terrorist Plots,” in Proc AAAI Conference on Artificial Intelligence, Phoenix, Arizona, USA, February 12–17, 2016 (2016) (CA, USA: AAAI), 30.
24. G L, Nemhauser L, WolseyM A. *An Analysis of Approximations for Maximizing Submodular Set Functions—I*. Germany: Mathematical Programming (1978).
25. Holme P, Kim BJ, Yoon CN, Han SK. Attack Vulnerability of Complex Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2002) 65:056109. doi:10.1103/PhysRevE.65.056109
26. Tsai J, Yin Z, Kwak JY, Kempe D, Tambe M. *Urban Security: Game-Theoretic Resource Allocation in Networked Physical domainsTwenty-Fourth Aaai Conference on Artificial Intelligence* (2011).
27. Motter AE, Lai YC. Cascade-based Attacks on Complex Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2002) 66:065102. doi:10.1103/PhysRevE.66.065102
28. Zhao L, Park K, Lai YC. Attack Vulnerability of Scale-free Networks Due to Cascading Breakdown. *Phys Rev E Stat Nonlin Soft Matter Phys* (2004) 70: 035101. doi:10.1103/PhysRevE.70.035101
29. Holmgren AJ. Using Graph Models to Analyze the Vulnerability of Electric Power Networks. *Risk Anal* (2006) 26:955–69. doi:10.1111/j.1539-6924.2006.00791.x
30. Nguyen DT, Shen Y, Thai MT. Detecting Critical Nodes in Interdependent Power Networks for Vulnerability Assessment. *IEEE Trans Smart Grid* (2013) 4:151–9. doi:10.1109/tsg.2012.2229398
31. Duan B, Liu J, Zhou M, Ma L. A Comparative Analysis of Network Robustness against Different Link Attacks. *Physica A: Stat Mech its Appl* (2016) 448: 144–53. doi:10.1016/j.physa.2015.12.045
32. Nguyen Q, Pham HD, Cassi D, Bellingeri M. Conditional Attack Strategy for Real-World Complex Networks. *Physica A: Stat Mech its Appl* (2019) 530: 121561. doi:10.1016/j.physa.2019.121561
33. Deng Y, Wu J, Tan YJ. Optimal Attack Strategy of Complex Networks Based on Tabu Search. *Physica A: Stat Mech its Appl* (2016) 442:74–81. doi:10.1016/j.physa.2015.08.043
34. Opsahl T. *The united states Air Transportation Network* (2007). Available at: https://toreopsahl.com/datasets/#usairports (Accessed June 23, 2021).

Conflict 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.

Publisher’s Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.