symmetry

MDPI

Article

Secure the IoT Networks as Epidemic Containment Game

Juntao Zhu [1], Hong Ding [1], Yuchen Tao [1], Zhen Wang [1] and Lanping Yu [2,*]

[1] School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China; zhujuntao@hdu.edu.cn (J.Z.); dinghong@hdu.edu.cn (H.D.); yuchen.tao@hdu.edu.cn (Y.T.); wangzhen@hdu.edu.cn (Z.W.)
[2] School of Information Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
* Correspondence: yulp@hdu.edu.cn

Abstract: The spread of a computer virus among the Internet of Things (IoT) devices can be modeled as an Epidemic Containment (EC) game, where each owner decides the strategy, e.g., installing anti-virus software, to maximize his utility against the susceptible-infected-susceptible (SIS) model of the epidemics on graphs. The EC game's canonical solution concepts are the Minimum/Maximum Nash Equilibria (MinNE/MaxNE). However, computing the exact MinNE/MaxNE is NP-hard, and only several heuristic algorithms are proposed to approximate the MinNE/MaxNE. To calculate the exact MinNE/MaxNE, we provide a thorough analysis of some special graphs and propose scalable and exact algorithms for general graphs. Especially, our contributions are four-fold. First, we analytically give the MinNE/MaxNE for EC on special graphs based on spectral radius. Second, we provide an integer linear programming formulation (ILP) to determine MinNE/MaxNE for the general graphs with the small epidemic threshold. Third, we propose a branch-and-bound (BnB) framework to compute the exact MinNE/MaxNE in the general graphs with several heuristic methods to branch the variables. Fourth, we adopt NetShiled (NetS) method to approximate the MinNE to improve the scalability. Extensive experiments demonstrate that our BnB algorithm can outperform the naive enumeration method in scalability, and the NetS can improve the scalability significantly and outperform the previous heuristic method in solution quality.

Keywords: cyber-security; epidemic control; game theory; complex network

Citation: Zhu, J.; Ding, H.; Tao, Y.; Wang, Z.; Yu, L. Secure the IoT Networks as Epidemic Containment Game. *Symmetry* **2021**, *13*, 156. https://doi.org/10.3390/sym13020156

Received: 8 January 2021
Accepted: 18 January 2021
Published: 20 January 2021

1. Introduction

Diffusion processes in small networks can model the explosive spread of computer viruses (e.g., WananCry ransomware 2017 [1]) in an IoT network or Cyber–Physical Systems (CPS) network. Efficient investment (secure firewall, etc.) can contain the spread of such adverse events, which involves a specific cost for individuals. Most owners of a device prefer to benefit from their neighbors as their security depends on the strategies of the entire population. These dilemmas with the following properties can be modeled as Interdependent Security (IDS) games: (1) a bad event happens suddenly within a population of devices, whose security depends on the entire population; (2) individuals can reduce these risks by the investment [2].

Researches propose many models in this area [3–6]. A large part of models involve individual utility functions that are difficult to compute, and some models cannot be extended to heterogeneous networks, which are not close to realistic scenarios. Thus, Saha et al. [7] used the characterization of spectral radius to simplify the utility function, and present a general dynamics SIS model for arbitrary graphs as an Epidemic Containment (EC) game. When an epidemic dies out in an EC game, every individual prefers not to change its strategy under a Nash Equilibrium (NE).

The study of computing equilibria is challenging. Minimum Nash Equilibria (MinNE) and Maximum Nash Equilibria (MaxNE) are essential parts of understanding NE. Several algorithms can be used to find MinNE/MaxNE for the EC game. High Degree (HDG) and Low Degree (LDG) are heuristic algorithms for MinNE and MaxNE, respectively [7].

They generate the strategy in a degree order, which will pick a node that does not belong to any secured node set of MinNE/MaxNE, leading to a big loss with the exact solution. Neighbors Information (NI) [8] is a heuristic MaxNE algorithm which performs better. NI decides with too much information: information of nodes, strategy of their neighborhood, and spectral radius of networks. On the one hand, the algorithms mentioned above perform poorly, as shown in Section 3. On the other hand, big complex networks are hard to estimate NE cost. Thus, company managers are interested in the small networks in which LDG/HDG/NI cannot give the exact MinNE/MaxNE.

To fill this gap, we provide a thorough analysis of some special graphs and propose exact and scalable algorithms for general graphs, and our contributions are four-fold. First, we give the MinNE/MaxNE for EC on special graphs based on spectral radius. For several important classes of network topologies (star-shaped graphs, complete graphs, and path graphs), MinNE and MaxNE are equal in most cases. Second, we provide an integer linear programming formulation (ILP) to compute MinNE/MaxNE for the general graphs with the small epidemic threshold. Third, we propose a Branch-and-Bound (BnB) framework to compute the exact MinNE/MaxNE in the general graphs with several heuristic methods to branch the variables. We speed up the search with information of degree, reduction of spectral radius, and neighborhood of nodes. We also adopt the NetShiled (NetS) method to approximate the MinNE to improve the scalability. Fourth, we test our methods empirically by comparing our algorithms with the enumeration method on a random tree, Erdős–Rényi (ER) random networks, and Barabási–Albert (BA) scale-free networks, and extensive experiments demonstrate that our algorithm framework can outperform the naive enumeration method in scalability. The NetS algorithm can improve the scalability significantly and outperform previous heuristic method in solution quality.

2. Related Work

Security game is a game-theoretic model that captures essential characteristics of decision making to protect and self-insure resources within a network [9]. Kumar et al. [10] limit the amount of graph information needed in the utility function, and consider decisions restricted to the graph induced by nodes within a distance. Jiang et al. [11] consider a network security game where the utility function determine by a weighted topology which represents the positive externality between players. The utility function in the EC game also involves a global quantity in the form of the spectral radius, which can be a good proxy for estimating this cost from the characterization of Ganesh et al. [6]. Secure problems (infection, computer virus, etc.) with interdependent actions can formulate as Interdependent Security (IDS) games [12,13]. Kunreuther et al. [14] mainly focus on the IDS game limited to the simple case of two agents. Moreover, general IDS model makes decisions on the one-hop strategy limiting the information as a system. Aspnes et al. [5] give an inoculation game model, which is a propagation-based IDS assuming a restricted network topology. In this study, the infected individual will infect all its neighbors. In the EC game, the individual is cured with a fixed rate. It is more closely to the spread of epidemics in real life.

In the domain of immunization algorithm, Briesemeister et al. [15] give the random wiring immunization, which is typically overwhelmed on power-law graphs. Madar et al. [16] present an "acquaintance" immunization policy that picks a random person and immunizes one random neighbor. The analytical result shows that it is better than several immunization policies for scale-free graphs. Chen et al. [17] give an approximate algorithm (NetShiled) to immunize the top k node, using matrix perturbation theory to approximate the drop of the spectral radius. Some similar works also focus on an efficient vaccination algorithm without considering NE structure [18,19]. To find NE in EC game, High Degree (HDG) and Low Degree (LDG) [7] give a rough approximation for MinNE and MaxNE by picking nodes in degree orders and checking in reverse degree orders, respectively. Xu et al. [8] find that LDG performs poorly with small network scope, and gives a heuristic algorithm with neighbors' degree and strategy. Saha et al. [20] propose GreedyWalk, which reduces

the spectral radius by reducing the number of closed walks of length k. It spends too much time to determine the closed walks. However, all the works cannot give exact MinNE/MaxNE even in small networks.

3. Preliminaries

The Epidemic Containment (EC) game [7] is based on an undirected graph $G(V, E)$ with the node set V and the edges set E. We use i as the index of the node, $i = 0, \ldots, N-1$, $N = |V|$. The neighbor set is denoted by $N(i)$ and $\boldsymbol{A}(G)$ denotes the the adjacency matrix of G. An example of an Epidemic Containment (EC) game can be shown in Figure 1.

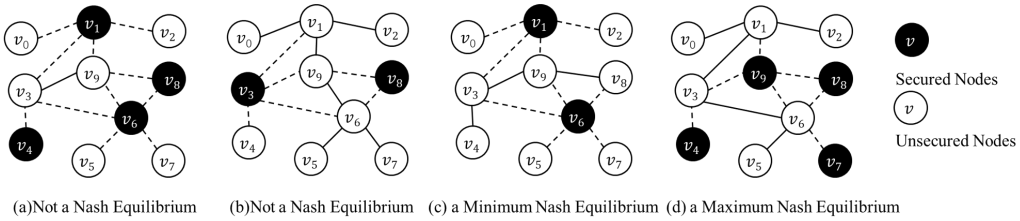

Figure 1. An Example of an Epidemic Containment (EC) game $\lambda_1 = 3.23$, $T = 2$. (**a**) One kind of non-Nash Equilibria (NE) where $\lambda_1 = 1 < T$ but when some nodes change their strategies it still has $\lambda_1 < T$, $\mathbf{a}_a = (0,1,0,0,1,0,1,0,1,0)$, $S_a = \{1,4,6,8\}$. The spectral radius is determined by $G_3[V - S(\mathbf{a}_a)]$ and $\lambda_1(G_3[V - S_a]) = 1 < T$, $c_0(\mathbf{a}_a) = C_0$, $c(\mathbf{a}_a) = 6C_0 + 4C_1 = 4$. If node 8 switches its strategy from $a_8 = 1$ to $a'_8 = 0$, reducing cost from C_1 to C_0, we get $\mathbf{a}'_a$ and S'_a. Now that $\lambda_1(G_8[V - S'_a]) = \sqrt{2} < T$ and epidemic still dies out, $\mathbf{a}_a$ is not NE. (**b**) Another kind of non-Nash Equilibria in which $\lambda_1 = 2.3 > T$ epidemic will spread around. (**c**) A Minimum Nash Equilibria with $c(\mathbf{a}_c) = 2, \lambda_1 = 1.618$. If nodes 1 or 6 change their strategy, the epidemic spreads out. In addition, it is safe for the rest graph immunized from the secured node. We cannot find another NE strategy with a cost lower than $c(\mathbf{a}_c)$. (**d**) A Maximum Nash Equilibria with $c(\mathbf{a}_d) = 4$, $\lambda_1(G_1[V - S(\mathbf{a}_d)]) = 1.902 < T$. No node can benefit from changing its strategy and there is no strategy with a cost bigger than $\mathbf{a}_d$.

Epidemic Model. We choose a spectral characterized susceptible-infected-susceptible (SIS, developed by Ganesh et al. [6]) model as epidemic model. In the SIS model, nodes are in states susceptible (S) or infected (I). Initially, some source nodes get infected, and all other nodes are susceptible. Each infected node i infects each of its neighbors j currently in state S at a transmission rate β; if neighbor j gets infected, it switches to state I. Each infected node i switches back to state S at rate δ. An epidemic dies out soon if $\lambda_1(G) < \delta/\beta$, where $\lambda_1(G)$ is the spectral radius of the contact graph G or the largest eigenvalue of the $\boldsymbol{A}(G)$. We define $T = \delta/\beta$ as the threshold which is smaller than $\lambda_1(G)$, and $\lambda_1(G) \geqslant T$ implies the epidemic lasts long [7,21].

Game Model. Let a_i denote the discrete strategy selected by the node i independently, whether to become secured (denoted by $a_i = 1$) or not (denoted by $a_i = 0$). $\mathbf{a} = \{a_0, a_1, \ldots, a_{N-1}\}$ denotes the strategy profile of all the nodes. We use $\mathbf{a}_{-i}$ to denote the strategy profile of the players other than node i. $S(\mathbf{a}) = \{i \in V : a_i = 1\}$ denotes secured node set with the strategy profile $\mathbf{a}$, and the graph $G[V - S(\mathbf{a})]$ induced by the set $V - S(\mathbf{a})$ of unsecured nodes called attack graph. $G_i[V - S(\mathbf{a})]$ represents the unique connected component of $G[V - S(\mathbf{a})]$ that contains node i. A node will incur a cost C_1 (the cost for a vaccination), if node i chooses to be secured, i.e., $a_i = 1$. If node i is not secured, i.e., $a_i = 0$, it probably gets infected, and its cost depends on whether or not the epidemic dies out quickly in the connected component induced by the unsecured nodes. If $\lambda_1(G_i[V - S(\mathbf{a})]) < T$, node i merely bears a cost C_0 (the cost of secured by its neighbor); if $\lambda_1(G_i[V - S(\mathbf{a})]) \geqslant T$, node i in the susceptible state will suffer the cost C_2 (the cost

of recovery, $C_0 < C_1 < C_2$). Given the strategy profile $\mathbf{a}$, the cost of each node $c_i(\mathbf{a})$ is described as below:

$$c_i(\mathbf{a}) = \begin{cases} C_0, & a_i = 0\ ,\ \lambda_1(G_i[V - S(\mathbf{a})]) < T; \\ C_1, & a_i = 1; \\ C_2, & a_i = 0\ ,\ \lambda_1(G_i[V - S(\mathbf{a})]) \geqslant T. \end{cases} \tag{1}$$

$c(\mathbf{a}) = \sum_{i \in V} c_i(\mathbf{a})$ is the cost of strategy $\mathbf{a}$. Nash Equilibrium is defined as below:

Definition 1. *For a strategy profile* $\mathbf{a}$, $\forall i \in V$, *we have* $\mathbf{a}'$ *in which* a_i' *is the alternative strategy for node* i *and* $a_j' = a_j, \forall i \neq j$. *The strategy profile* $\mathbf{a}$ *is Nash Equilibrium (NE) in EC game if and only if* $c_i(\mathbf{a}) \leqslant c_i(\mathbf{a}'), \forall i \in V$.

In an NE, node i cannot benefit by changing its strategy, given that $\mathbf{a}_{-i}$ is fixed [7]. If $\mathbf{a}$ is NE, $C_{Min} = min\, c(\mathbf{a})$ is the cost of Minimum Nash Equilibria (MinNE), and $C_{Max} = max\, c(\mathbf{a})$ is the cost of Maximum Nash Equilibria (MaxNE). There is an example of EC game under $T = 2.0$. An instance of EC game can be defined as a tuple $EC(G, T, C_0, C_1, C_2)$. For the rest of the paper, we will focus on instances where $C_0 = 0$, $C_1 = 1$ and $C_2 = 2$. Computing the Minimum Nash Equilibria (MinNE) is NP-complete [7]. We can prove complexity of Maximum Nash Equilibria (MaxNE) is NP-complete in the same way.

Lemma 1. *Finding the Maximum Nash Equilibria of an EC game is NP-complete.*

Proof. To prove this statement, we reduce the problem of finding vertex cover to this problem. Let I_{VC} and I_{EC} be two general instances of the two problems defined as follows: (1) $I_{VC}(G^{'}, P^{'})$: Given a graph $G^{'} = (V, E)$, is there a vertex cover set of size $P^{'}$ or less? (2) $I_{EC}(G, T, C_0, C_1, C_2, P)$: Given the EC game (G, T, C_0, C_1, C_2), is there a configuration with social cost P or less? We reduce I_{VC} to I_{EC} as follows: set $G = G^{'}$, $T = \epsilon$, where ϵ is arbitrarily close to 0, set $C_0 = 0$, $C_2 = \infty$, choose C_1 such that $0 < C_1 < \infty$ and set $P = P^{'}C$. Clearly, the reduction takes polynomial time. Now we show this is a valid reduction. If there is a vertex cover set $V_1 \subset V$ of size $|V_1| = P$, then V_1 corresponds to a secured node set of I_{EC} yielding social cost $P = P^{'}C_1$. As a result that removing the vertex cover set, by definition, leaves no edge in the graph and so, the spectral radius of the attack graph is 0 which is less than ϵ. Therefore, all the unsecured nodes incur zero cost and NE cost is $P = P^{'}C_1$. On the other hand, if there is a secured node set $V_1 \subset V$ of cardinality $|V_1| = P$, and NE cost $P^{'}C_1$ in I_{EC}, that means removing V_1 from G, leaves no edge in the graph. By definition, V_1 is a vertex cover to G of size P. Therefore, this is a valid polynomial time reduction and finding the corresponding social cost with P in EC game is NP complete. Set $P = |V| - 1, \ldots, 1$ in a decreasing order, the first answer for I_{VC} is the MaxNE for the corresponding I_{EC}. □

4. Counterexample for HDG/LDG/NI

ITERATIVESECURE (IS) [7] is a method to generate an NE for the EC game with two nodes permutations π and ρ. HDG/LDG/NI [7,8] is based on ITERATIVESECURE and designed to obtain approximate MinNE or MaxNE for the EC game. According to nodes permutation π in V, ITERATIVESECURE produces a secured node set S, and ends with $\lambda_1(G_i[V - S]) < T$, $i \in V - S$. Then, ITERATIVESECURE checks every node in set S by a nodes permutation ρ in V. If node $\rho(i)$ changes its strategy $\lambda_1(G_{\rho(i)}[V - (S - \rho(i))]) < T$, delete the node from S. Permutation of nodes π and ρ in HDG are non-increasing and non-decreasing degree orders. LDG is also based on ITERITERATIVESECURE [7], permutation π and ρ are non-decreasing and non-increasing degree orders. In NI, permutation π and ρ are non-decreasing and non-increasing score orders. They have similar disadvantages: (1) pick a node too early but fail to delete it from the S (e.g., node 4 in Figure 2a); (2) fail to reach a node in permutation π which is necessary for NE (e.g., node 4 in Figure 2c); (3)

confuse the nodes with the same property (degree, reduction of spectral radius, etc.). Thus, previous algorithms cannot give the exact MinNE/MaxNE even in small networks, and we propose some algorithms to find exact MinNE/MaxNE.

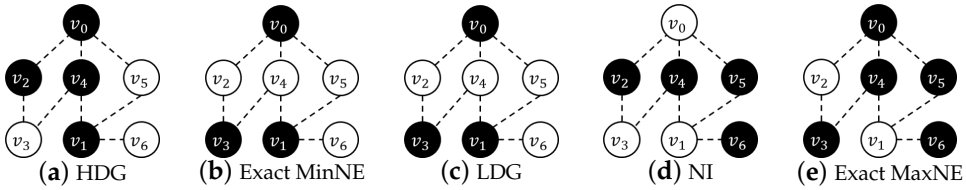

Figure 2. A network for EC game with $N = 7$, $T = 1.0$. (**a**) High Degree (HDG) picks nodes in non-increasing degree order with permutation $\{0, 1, 4, 2\}$, and check nodes with permutation $\{2, 4, 1, 0\}$. (**a**) HDG gets an NE with $c = 4$ as MinNE, when exact MinNE (**b**) is $c = 3$ with $\{0, 1, 3\}$. (**c**) Low Degree (LDG) picks nodes in non-decreasing degree order with permutation $\{6, 2, 3, 5, 0, 1\}$, and check nodes with permutation $\{1, 0, 5, 3, 2, 6\}$. LDG gets an NE with $c = 3$ as MinNE, NI (**d**) gets an NE with $c = 4$, when exact MaxNE (**e**) is $c = 5$ with $\{0, 3, 4, 5, 6\}$.

5. Approach to Find Nash Equilibria for Special Networks

In this section, we explore the NE based on characters of spectral radius for three network typologies: star-shaped graphs, complete graphs, and path graphs. Given the threshold T and a specific graph, we can give a strategy and find that MinNE/MaxNE are equal in some cases.

5.1. Star-Shaped Networks

The spreading on a large amount of power-law graphs is often determined by the spreading on the star-shaped subgraphs [6]. A star-shaped graph S_N is a graph with N nodes where the only edges are $(0, i)$, $i = 1, \ldots, N-1$. The spectral radius of a star-shaped graph S_k is $\lambda_1(S_k) = \sqrt{N}$ [6]. Node $i = 1, \cdots, N-1$ has the same structure. When $1 < T$ and $\sqrt{k} < T \leqslant \sqrt{k+1}$, $|N-k-1|$ nodes around node 0 getting secured can reach an NE and $C_{Min} = C_{Max} = N-k-1$. However, for $0 < T \leqslant 1$, we have $C_{Min} = 1$ to immunize node 0 and $C_{Max} = N-1$ to immunize the other nodes, respectively.

5.2. Complete Graph

The complete graph also plays a prominent role in networks. For example, the BGP routers, belonging to the Internet's top-level autonomous systems, form an utterly connected component [6]. A complete graph K_N is a connected graph with N vertices where all vertices are of degree $N-1$. When the network is a complete graph, we have spectral radius $\lambda_1(K_N) = N-1$ [22]. A complete graph is a homogeneous network, and every node has the same importance to getting secured. No node needs to be secured under $N-1 < T$. For $0 < T \leqslant N-1$, we can reach NE by randomly picking $N - \lfloor T \rfloor$ nodes to immunize, $C_{Min} = C_{Max} = N - \lfloor T \rfloor$.

5.3. Path Graphs

Paths graphs are simple and often crucial in their role as subgraphs of other graphs. A path graph P_N is a graph whose vertices can be listed in the order $0, 1, \cdots, N-1$ such that the edges are $(i, i+1)$ where $i = 0, 1, \cdots, N-2$. The spectral radius of a path graph P_N is $\lambda_1(P_N) = 2 \cdot cos(\frac{\pi}{N+1}) < 2$ [23]. A path graph P_N has 2 pendant nodes and the other $N-2$ nodes of degree 2 which have similar importance. When $2 \cdot cos(\frac{\pi}{k}) < T \leqslant 2 \cdot cos(\frac{\pi}{k+1})$, MinNE immunize last node every $k+1$ nodes, $C_{Min} = \lfloor \frac{N}{k+1} \rfloor$. Under this threshold, MaxNE immunize two nodes every $k+2$ nodes in a fixed order, $C_{Max} = 2 \cdot \lfloor \frac{N}{k+2} \rfloor + \lfloor \frac{N \bmod (k+2)-1}{k} \rfloor$.

6. Approach to Find Nash Equilibria for Small Threshold

We obtain MinNE/MaxNE structure based on the threshold for specific network topology. We find that it is a minimum vertex cover problem in the case ($T \leqslant 1$) to finding MinNE. We extend integer linear programming formulation to finding MinNE/MaxNE in threshold $0 < T \leqslant 1$, and $1 < T \leqslant \sqrt{2}$.

6.1. MinNE/MaxNE for $T \leqslant 1$

When $T \leqslant 1$, it is a minimum vertex cover problem to finding MinNE. We can compute MaxNE by adding a constraint of neighborhood number. Every node is isolated from each other under this threshold, and spectral radius of graph $\lambda_1(G[V - S(\mathbf{a})])$ is 0.

Proposition 1. *When threshold is small ($T \leqslant 1$), a strategy profile* $\mathbf{a}$ *is NE that every node is isolated from each other.*

Proof. Every edge with two unsecured nodes ($a_i = 0$) gets $\lambda_1 = 1 > T$. Strategy $\mathbf{a}$ is not an NE in which epidemic lasts long. In other words, every edge has at least one node $a_i = 1$ immune to decline the $\lambda_1 = 0 < T$. □

For a minimum vertex cover problem, MinNE can be formulated as Equation (2) according to Proposition 1. $1 \leqslant a_i + a_j \leqslant 2$ ensures Proposition 1 that every edge can immunize one node or two nodes.

$$\min \sum_{i=0}^{N-1} a_i, \tag{2a}$$

$$1 \leqslant a_i + a_j \leqslant 2,\ \forall (i,j) \in E, a_i \in \{0,1\}. \tag{2b}$$

To reach the MaxNE, we maximize $\sum_{i=0}^{N-1} a_i$. What is different from MinNE is Equation (3c). This constraint ensures at least one node around $i \in N(j)$ including itself not get secured. Otherwise, it is not an NE that node j can change its strategy to $a_j = 0$. The MaxNE with threshold $0 < T \leqslant 1$ can be formulated as Equations (3a)–(3c).

$$\max \sum_{i=0}^{N-1} a_i, \tag{3a}$$

$$1 \leqslant a_i + a_j \leqslant 2,\ \forall (i,j) \in E, \tag{3b}$$

$$a_j + \sum_{i \in N(j)} a_i \leqslant |N(j)|, a_i \in \{0,1\}. \tag{3c}$$

6.2. MinNE/MaxNE for $1 < T \leqslant \sqrt{2}$

For $1 < T \leqslant \sqrt{2}$, we extend the integer linear programming formulation for MinNE/MaxNE from $T < 1$. The maximum connected component in the graph is an edge with two nodes, and spectral radius of graph $\lambda_1(G[V - S(\mathbf{a})])$ is 1 in this situation.

Proposition 2. *When a strategy profile* $\mathbf{a}$ *is an NE under $1 < T \leqslant \sqrt{2}$, the maximum connected component in $G[V - S(\mathbf{a})]$ is a line with two unsecured nodes assuming G has at least one edge.*

Proof. Edge with two unsecured nodes ($a_i = 0$) gets $\lambda_1 = 1.0$. For $1 < T \leqslant 1.414$, maximum connected component in $G[V - S(\mathbf{a})]$ is three nodes with two edges $\lambda_1 = 1.414$, and epidemic lasts long. Hence, $\mathbf{a}$ has maximum connected component containing no more than three nodes. On the other hand, $G[V - S(\mathbf{a})]$ has a edge (i,j) with one secured end node i, $a_i = 1$, $a_j = 0$, $\lambda_1(G[V - S(\mathbf{a})]) = 0$. Node i can change its strategy $x_i' = 0$ that $\lambda_1(G[V - S(\mathbf{a}')]) = 1.0 < T$. Therefore, $\mathbf{a}$ is NE, the maximum connected component in $G[V - S(\mathbf{a})]$ is a edge. □

Secured nodes consider to minimize the cost for MinNE. Every susceptible node i has at most one susceptible neighbor node j, $a_j = 0$, $j \in N(i)$. Equation (4b) ensures

the maximum connected component in the graph is one edge with two unsecured nodes according to Proposition 2.

$$\min \sum_{i=0}^{N-1} a_i, \tag{4a}$$

$$(1-a_i)+(1-a_i)\cdot\sum_{j\in N(i)}(1-a_j)\leqslant 2, a_i\in\{0,1\}. \tag{4b}$$

We reformulate Equations (4a) and (4b) to find MinNE by maximizing $\sum_{i=0}^{N-1} z_i$, where $z_i = 1-a_i, i = 0,\ldots,N-1$. To solve the problem as ILP, we introduce w_{ij} to describe the relationship between a_i and a_j, $(i,j)\in E$.

$$\max \sum_{i=0}^{N-1} z_i, \tag{5a}$$

$$z_i+\sum_{j\in N(i)} w_{ij}\leqslant 2, z_i+z_j-w_{ij}\leqslant 1, \tag{5b}$$

$$w_{ij}\leqslant z_i, w_{ij}\leqslant z_j, z_i\in\{0,1\}, w_{ij}\in\{0,1\}. \tag{5c}$$

We can find MaxNE by minimizing $\sum_{i=0}^{N-1} z_i$ with Equations (6a)–(6c). Equation (6b) makes sure every node, whether secured or not, at least has one unsecured neighbor. Equations (6c) and (6d) satisfy Proposition 2.

$$\min \sum_{i=0}^{N-1} z_i, \tag{6a}$$

$$1\leqslant\sum_{j\in N(i)} z_j,\ \forall 1\leq|N(i)|, \tag{6b}$$

$$z_i+\sum_{j\in N(i)} w_{ij}\leqslant 2, z_i+z_j-w_{ij}\leqslant 1, \tag{6c}$$

$$w_{ij}\leqslant z_i, w_{ij}\leqslant z_j, z_i\in\{0,1\}, w_{ij}\in\{0,1\}. \tag{6d}$$

7. Approach to Find Nash Equilibria for General Networks

To solve MinNE/MaxNE for the general networks, we first propose an enumeration method to solve the problem. Enumeration becomes time-consuming as node number increasing. We propose a Branch-and-Bound (BnB) algorithm to tackle it with several ways to improve searching speed and scalability. Our BnB speed up the search in degree order, reduction of spectral radius, and neighborhood information. Finally, NetS improves the scalability of our algorithm framework for approximation.

7.1. Enumeration

Enumeration (Enum) is brute force algorithm to find all the MaxNE/MinNE and helps visualizing the structure when the network is small. Let $\mathbf{a}^B$ denote strategy with the strategy index B, which satisfies that $B=\sum_{i=0}^{N-1} 2^i\cdot a_i^B$, $|\mathbf{X}|=2^N$.

Here we merely give the Enum (Algorithm 1) to find all MaxNE. In step 1, Enum calculates all the $\mathbf{a}\in\mathbf{X}$, index of $\boldsymbol{B}$, and corresponding spectral radius $\lambda_1(G[V-S(\mathbf{a}^B)])$ and cost $c(\mathbf{a}^B)$. In steps 2–4, Enum finds all the MaxNE with specific threshold T according to the definition of NE. Finding MinNE is to change the judging criterion in step 2 and record the cost of MinNE C^*_{Min} instead.

Algorithm 1: Enum.

Input: Graph $G(V,E)$, threshold of epidemic T
Output: A set S_X of strategies for MaxNE
1 $\forall\mathbf{a}\in\mathbf{X}$, we get B to calculate $\lambda_1(\mathbf{a}^B)$ and $c(\mathbf{a}^B)$, $S_X=\emptyset$, $C^*_{Max}=0$;
2 **foreach** $\mathbf{a}^B\in\mathbf{X}$, $\lambda_1(\mathbf{a}^B)<T$ *and* $\mathbf{a}^B$ *is NE* **do**
3 **if** $c(\mathbf{a}^B)>C^*_{Max}$ **then** $S_X=\{\mathbf{a}^B\}$, $C^*_{Max}=c(\mathbf{a}^B)$;
4 **if** $c(\mathbf{a}^B)=C^*_{Max}$ **then** $S_X=S_X+\{\mathbf{a}^B\}$;

7.2. Branch-and-Bound

We develop an efficient Branch-and-Bound (BnB) algorithm (Algorithm 2) to search the exact MinNE/MaxNE in strategy profile space $\mathbf{X}$ ($|\mathbf{X}| = 2^N$).

Branch. For every node at level i (according to nodes permutation π) of the search tree, we have a corresponding pair $(a^-_{\pi_i}, a^+_{\pi_i})$, $a^-_{\pi_i} = 0$, $a^+_{\pi_i} = 1$. At every node π_i, the tree is expanded by performing a branching operation. Two nodes are introduced: a left node where $\mathbf{a}^* = \mathbf{a}^* + \{a^-_{\pi_i}\}$ and a right node where $\mathbf{a}^* = \mathbf{a}^* + \{a^+_{\pi_i}\}$. The check of NE in leaves is irreplaceable, and original BnB uses a random nodes permutation π. We can choose an order to search the tree (node permutation π). In this way, it is possible to find a MinNE earlier. We proposed BnB-D/BnB-E/BnB-N from three different perspectives and speed up the pruning.

Algorithm 2: Branch-and-Bound for MinNE.

Input: Graph $G(V, E)$, threshold T, permutation π
Output: Set of secure nodes $S(\mathbf{a})$

1 get MinNE upper bound cost C^*_{Min} from HDG; $i = 0$, $\mathbf{a}^* = \{a^-_{\pi_0}\}$, $isSearch = true$;
2 **while** $\pi_i \in V$ **do**
3 **if** π_i *is the last node* **then**
4 **if** $c(\mathbf{a}^*) < C^*_{Min}$ *and* $\mathbf{a}^*$ *is NE* **then** $\mathbf{a} = \mathbf{a}^*$, $C^*_{Min} = c(\mathbf{a}^*)$;
5 **if** $a^*_{\pi_i} = a^-_{\pi_i}$ **then**
6 $a^*_{\pi_i} = a^+_{\pi_i}$;
7 **if** $c(\mathbf{a}^*) < C^*_{Min}$ *and* $\lambda_1(G[V - S(\mathbf{a}^*)]) < T$ **then** $\mathbf{a} = \mathbf{a}^*$, $C^*_{Min} = c(\mathbf{a}^*)$;
8 $\mathbf{a}^* = \mathbf{a}^* - \{a_{\pi_i}\}$, $i = i - 1$, $isSearch = false$;
9 **else**
10 **if** *isSearch* **then**
11 $\bar{\mathbf{a}} = \mathbf{a}^* + \{a^+_{\pi_{i+1}}, \cdots, a^+_{\pi_{N-1}}\}$, $\underline{\mathbf{a}} = \mathbf{a}^* + \{a^-_{\pi_{i+1}}, \cdots, a^-_{\pi_{N-1}}\}$;
12 **if** $c(\underline{\mathbf{a}}) < C^*_{Min}$ *and* $\lambda_1(G[V - S(\bar{\mathbf{a}})] < T$ **then** $i = i + 1$, $\mathbf{a}^* = \mathbf{a}^* + \{a^-_{\pi_i}\}$;
13 **else** $isSearch = false$;
14 **else**
15 **if** $a^*_{\pi_i} = a^-_{\pi_i}$ **then** $a^*_{\pi_i} = a^+_{\pi_i}$, $isSearch = true$;
16 **else** $\mathbf{a}^* = \mathbf{a}^* - \{a_{\pi_i}\}$, $i = i - 1$;

(i) Degree order: Immunizing large degree nodes helps BnB find MinNE more quickly. For BnB-D, we use a non-increasing degree order permutation $\{\pi_0, \pi_1, \pi_2, \ldots, \pi_{N-1}\}$, $d(\pi_0) \geqslant d(\pi_1) \geqslant \cdots \geqslant d(\pi_{N-1})$.

(ii) Reduction of spectral radius: In our model, we compare spectral radius with threshold to determine epidemic dies out or not. Therefore, reducing spectral radius seems to be efficient to control epidemic. We adopt BnB-E based on drop of spectral radius orders, $\Delta\lambda_1(i) = \lambda_1(G) - \lambda_1(G[V - S_{\mathbf{a}}])$, node i is only node secured in $\mathbf{a}$. We have permutation $\{\pi_0, \pi_1, \pi_2, \ldots, \pi_{N-1}\}$, $\Delta\lambda_1(\pi_0) \geqslant \Delta\lambda_1(\pi_1) \geqslant \cdots \geqslant \Delta\lambda_1(\pi_{N-1})$.

(iii) Neighborhood information: We find that secured node i will bring benefit for its neighborhood, i.e., its neighbor is more likely to not vaccinate. The BnB-N searches in nodes permutation that there are node π_i and its adjacent node π_j, $\pi_j \notin N(\pi_i)$. We have permutation $\{\pi_0, \pi_1, \pi_2, \ldots, \pi_{N-1}\}$ that edge $(\pi_i, \pi_{i+1}) \notin E$,$i = 0, \cdots, N-2$.

Bound. BnB keeps track of bounds by two constraints. One is lower bound: the cost $c(\underline{\mathbf{a}})$ of current $\mathbf{a}^*$ should be less than C^*_{Min}, assuming all the rest nodes choose a^-, $\underline{\mathbf{a}} = \mathbf{a}^* + \{a^-_{\pi_{i+1}}, \cdots, a^-_{\pi_{N-1}}\}$. The other is upper bound: epidemic should not spread out even all the rest nodes choose to immunize themselves a^+, $\lambda_1(G[V - S(\bar{\mathbf{a}})] > T$, $\bar{\mathbf{a}} = \mathbf{a}^* + \{a^+_{\pi_{i+1}}, \cdots, a^+_{\pi_{N-1}}\}$. Only if the search reaches the leaves (all nodes have their strategy) can we check the strategy $\mathbf{a}^*$ is an NE with less cost $c(\mathbf{a}^*) < C^*_{Min}$.

In step 1, BnB (Algorithm 2) uses HDG [7] to get the upper bound of MinNE based on the breadth-first search (BFS). In steps 4–8, as every node has its strategy, BnB checks if $\mathbf{a}^*$ is a MinNE. In 10–13, BnB checks the upper bound $\bar{\mathbf{a}}$ and lower bound $\underline{\mathbf{a}}$ of node i and decides to bound it or not. In 15–16, BnB changes searching nodes from left nodes to

the right nodes and right nodes to its parent node. When the searching process finished, strategy **a** is a MinNE.

7.3. NetShiled (NetS)

Finding a MinNE in the EC game can be divided into two steps:(1) finding an optimal set or permutation of nodes whose removal would maximally reduce the spectral radius of the network; (2) checking the set of the immunized nodes to NE for EC game.

For the first step, we can find the key nodes by circulating the drop of eigenvalue $\Delta\lambda_1$ when deleting the set of nodes S from the original graph G, $\Delta\lambda_1 = \lambda_1(G) - \lambda_1(G[V-S])$. As the size of nodes increases, computing the drop of eigenvalue $\Delta\lambda_1$ is more difficult.

The NetShield [17] uses Shield-value score $Sv(S)$ to precisely approximate the drop of eigenvalue $\Delta\lambda_1$ by matrix perturbation theory. The original NetShield merely finds k nodes to immunize without taking equilibria into consideration. Therefore, we extend NetShield with ITERATIVESECURE to change strategy generated into equilibrium, called NetS (Algorithm 3). Let bold upper cases represent matrices, e.g., $\boldsymbol{A}$, $\boldsymbol{C}$. Bold lower cases stand for column vectors respectively, e.g., $\boldsymbol{u}$, $\boldsymbol{w}$. Let $\boldsymbol{u}_i$ denotes the ith eigenvector for matrix $\boldsymbol{A}$. Let $\boldsymbol{A}(i,:)$ denotes the ith row of matrix $\boldsymbol{A}$, and $\boldsymbol{A}(:,j)$ the jth column of matrix $\boldsymbol{A}$. $\boldsymbol{A}(:,S)$ denotes the matrix of $\boldsymbol{A}$ which contains columns in node set S. Shield-value score $Sv(S)$ is defined as:

$$Sv(S) = \sum_{i\in S} 2\lambda_1 \boldsymbol{u}(i)^2 - \sum_{i,j\in S} \boldsymbol{A}(i,j)\boldsymbol{u}(i)\boldsymbol{u}(j) \tag{7a}$$

$$\Delta\lambda_1 = Sv(S) + O(\sum_{j\in S} ||\boldsymbol{A}(;:j)||^2) \tag{7b}$$

We also have Equation (7b) justifying the precision of $Sv(S)$. Algorithm 3 computes the largest eigenvalue λ_1 and the corresponding eigenvector $\boldsymbol{u}$ in steps 1–2. In step 4, the value $\boldsymbol{w} = \{w_0, \cdots, w_{N-1}\}$ measures the Shield-value score of each individual node. Then, in each iteration of steps 6–11, NetS greedily select one more node and add it into set S according to $score(i)$ (step 10), generating the permutation π until $\lambda_1(G[V-S]) < T$. Note that steps 11–12 are to exclude those nodes that are already in the selected set S. Step 11 makes sure that strategy with immunization of S is an NE. The time complexity of Algorithm 3 is $\mathcal{O}(N^3 + |E|)$.

Algorithm 3: NetS.

Input: Graph $G(V,E)$, threshold of epidemic T
Output: A set of secure nodes S
1 compute the largest eigenvalue λ_1 of $\boldsymbol{A}$;
2 let $\boldsymbol{u}$ be the corresponding eigenvector of λ_1, $\boldsymbol{u}(i)(i = 0, \cdots, N-1)$ the ith value of $\boldsymbol{u}$;
3 $S = \emptyset$, permutation $\pi = \emptyset$;
4 **for** $i = 0$ *to* $N-1$ **do**
5 $\quad \boldsymbol{w}(i) = (2\cdot\lambda_1 - \boldsymbol{A}(i,i))\cdot\boldsymbol{u}(i)^2$;
6 **while** $\lambda_1(G[V-S]) \geq T$ **do**
7 $\quad$ let $\boldsymbol{C} = \boldsymbol{A}(:,S)$, $\boldsymbol{b} = \boldsymbol{C}\cdot\boldsymbol{u}(S)$;
8 $\quad$ **for** $i = 0$ *to* $N-1$ **do**
9 $\quad\quad$ **if** $i \in S$ **then** let $score(i) = -1$;
10 $\quad\quad$ **else** let $score(i) = \boldsymbol{w}(i) - 2\cdot\boldsymbol{b}(i)\cdot\boldsymbol{u}(i)$;
11 $\quad$ let $j = argmax_i score(i)$, $\pi = \pi + \{j\}$, $S = S \cup \{j\}$;
12 let $\rho = reverse\ \pi$, $i = 0$;
13 **foreach** $\lambda_1(G[V-(S-\{\rho(i)\})]) < T$ **do**
14 $\quad S = S - \{\rho(i)\}$;

8. Empirical Results

We evaluate the performance of our approach through extensive experiments. We use CPLEX (version 12.9) to solve all integer linear programs (ILP). All computations are performed on a PC with a 2.60 GHz quad-core CPU and 16.00 GB memory. All values averaged over 40 instances unless otherwise specified. We conduct experiments on three types of graph structures which widely used to model connections between population: (i) Random trees (RT), where every new node is attached to a randomly picked incumbent; (ii) Barabási–Albert scale-free model, which is denoted by BA(m) where m represents the average node degree; (iii) Erdős–Rényi random graphs, which is denoted by ER(p) where p represents the existence probability of an edge between any pair of nodes [24]. We use BA scale-free networks with parameters $m = 4, 6$, and use ER random graphs with parameters $p = 0.1, 0.2$.

We compare the scalability and optimality of four versions of algorithms: (i) ILP: integer linear programming for small threshold ($T \leqslant \sqrt{2}$); (ii) BnB: branch and bound algorithm with random searching permutation; (iii) BnB-D/BnB-E/BnB-N: BnB algorithm which searches with permutation base on the degree of nodes, eigenvalues drop of nodes and neighborhood information of nodes; (iv) NetS: heuristic algorithm which generates NE by a node permutation according to the drop of eigenvalue. We use Enum as a benchmark for exact solution, HDG as benchmark for approximation. The HDG algorithm is a heuristic algorithm that obtained MinNE by running the IS procedure with π and ρ permutations of nodes in non-increasing and non-decreasing degree orders.

Runtime. In Figure 3a–e,f–j, we compare the scalability of the proposed algorithms on 5 types of networks under $T = 1.0$ and $T = 0.5\lambda_1$, respectively. For small threshold ($T \leqslant \sqrt{2}$), ILP performs as fast as the heuristic algorithms. BnB-D/BnB-E/BnB-N are shown to improve the searching speed. BnB-D is better than BnB-E/BnB-N in BA scale-free network, and degree heterogeneity turns out to be extremely useful in searching. NetS extends the scalability of the algorithm as node size is increasing.

Solution Quality. We compare the cost of MinNE with HDG as the benchmark. The results are illustrated in Figure 3k–t, Enum/ILP/BnB give the exact NE. BnB-D works well under the small threshold and sparse network structure like the TR graph. NetS gives a near-optimal performance and outperforms HDG, especially under the larger threshold.

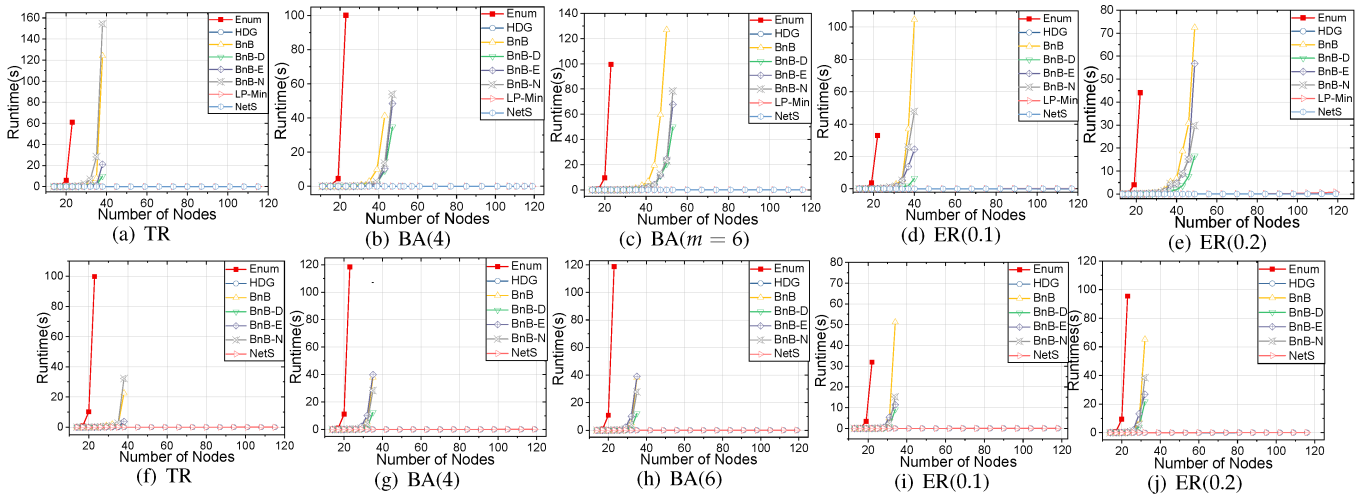

Figure 3. *Cont.*

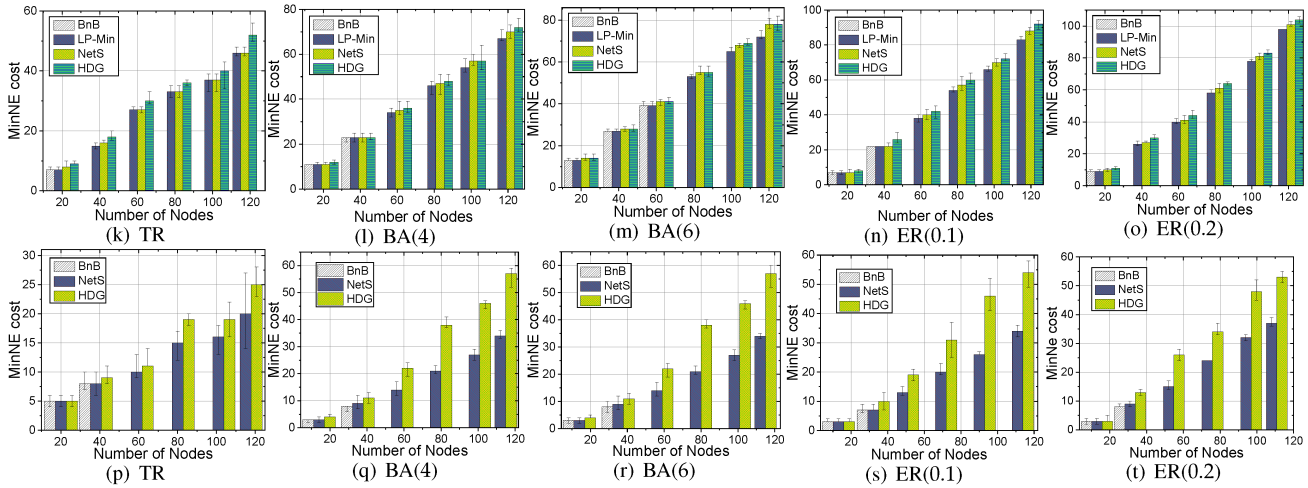

Figure 3. Scalability: (**a**–**e**), $T = 1.0$; (**f**–**j**), $T = 0.5\lambda_1$. Optimality: (**k**–**o**), $T = 1.0$; (**p**–**t**), $T = 0.5\lambda_1$.

9. Conclusions and Future Research

This paper focuses on exploring the Nash Equilibria in Epidemic Containment game, representing the spread of epidemics among interdependent users. As the most practical EC game application scenarios are IoT networks, we find that the previous algorithms (HDG/LDG/NI) cannot give exact MinNE/MaxNE in small networks.

To study the structure of exact NE, this paper first explores the network typologies' spectral radius. We can give the strategy directly for star-shaped graphs, complete graphs, and path graphs. By observing a single node's degree information, we propose linear programming formulations to finding the exact MinNE/MaxNE in threshold $0 < T \leqslant \sqrt{2}$ as quick as heuristic algorithms. Secondly, we develop an efficient Branch-and-Bound (BnB) algorithm branching with the degree information to speed up the research. To extend the algorithm's scalability, we propose the NetS which approximates the spectral radius's drop. This algorithm extremely outperforms HDG to find MinNE in larger Barabási–Albert and Erdős–Rényi random graphs. The following inspirations can be obtained from the experiment results: heterogeneity of degree and spectral radius turn out to be extremely useful for extracting information from nodes. However, our research is limited to artificial networks, and we get more information on the real-world networks, e.g., AS (Oregon-1), P2P (Gnutella-6) [19,25], which can help us extend our experiments to more realistic scenarios in the following researches.

In the future work, we would consider Stackelberg strategies to reduce MaxNE, a more realistic scenario. Combining IDS gaming security and data security concepts, we can also extend EC game on the relevant relationship networks with different granularity levels [26,27].

Author Contributions: J.Z., H.D., Y.T., Z.W., and L.Y. wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Zhejiang Provincial Natural Science Foundation of China under Grant Nos. LQY19G030001 and LY20F0300.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used during the study are available from the corresponding author.

Acknowledgments: The authors like to appreciate the referee for their valuable comments and suggestions.

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

References

1. Kumar, M.S.; Ben-Othman, J.; Srinivasagan, K.G. An Investigation on Wannacry Ransomware and its Detection. In Proceedings of the IEEE ISCC 2018, Natal, Brazil, 25–28 June 2018; pp. 1–6.
2. Heal, G.; Kunreuther, H. *Interdependent Security: A General Model*; Technical Report; National Bureau of Economic Research: Cambridge, MA, USA, 2004.
3. Omic, J.; Orda, A.; Van Mieghem, P. Protecting against network infections: A game theoretic perspective. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1485–1493.
4. Lelarge, M.; Bolot, J. A local mean field analysis of security investments in networks. In Proceedings of the 3rd International Workshop on Economics of Networked Systems, Seattle, WA, USA, 22 August 2008; pp. 25–30.
5. Aspnes, J.; Chang, K.; Yampolskiy, A. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *J. Comput. Syst. Sci.* **2006**, *72*, 1077–1093. [CrossRef]
6. Ganesh, A.; Massoulié, L.; Towsley, D. The effect of network topology on the spread of epidemics. In Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005; Volume 2, pp. 1455–1466.
7. Saha, S.; Adiga, A.; Vullikanti, A.K.S. Equilibria in epidemic containment games. In Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence, Quebec City, QC, Canada, 27–31 July 2014.
8. Xu, J.H.; Wang, Z.; Cui, G.H.; Ren, Y.Z.; Ding, H.; Choo, K.K.R. An Extended Exploration to the Epidemic Containment Game. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–7.
9. Grossklags, J.; Christin, N.; Chuang, J. Secure or insure: A game-theoretic analysis of information security games. In Proceedings of the 17th International Conference on World Wide Web, Beijing, China, 1 April 2008; pp. 209–218.
10. Kumar, V.A.; Rajaraman, R.; Sun, Z.; Sundaram, R. Existence Theorems and Approximation Algorithms for Generalized Network Security Games. In Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems, Genova, Italy, 21–25 June 2010; pp. 348–357.
11. Jiang, L.; Anantharam, V.; Walrand, J. Efficiency of selfish investments in network security. In Proceedings of the 3rd International Workshop on Economics of Networked Systems, Seattle, WA, USA, 22 August 2008; pp. 31–36.
12. Kearns, M.; Ortiz, L.E. Algorithms for interdependent security games. In Proceedings of the Advances in Neural Information Processing Systems, Vancouver, BC, Canada, 13–18 December 2004; pp. 561–568.
13. Heal, G.; Kunreuther, H. IDS models of airline security. *J. Confl. Resolut.* **2005**, *49*, 201–217. [CrossRef]
14. Kunreuther, H.; Heal, G. Interdependent security. *J. Risk Uncertain.* **2003**, *26*, 231–249. [CrossRef]
15. 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, 27 October 2003; pp. 67–75.
16. Madar, N.; Kalisky, T.; Cohen, R.; Ben-avraham, D.; Havlin, S. Immunization and epidemic dynamics in complex networks. *Eur. Phys. J. B* **2004**, *38*, 269–276. [CrossRef]
17. Chen, C.; Tong, H.; Prakash, B.A.; Tsourakakis, C.E.; Eliassi-Rad, T.; Faloutsos, C.; Chau, D.H. Node immunization on large graphs: Theory and algorithms. *IEEE Trans. Knowl. Data Eng.* **2015**, *28*, 113–126. [CrossRef]
18. Chen, W.; Wang, Y.; Yang, S. Efficient influence maximization in social networks. In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Paris, France, 28 June–1 July 2009; pp. 199–208.
19. Van Mieghem, P.; Stevanović, D.; Kuipers, F.; Li, C.; Van De Bovenkamp, R.; Liu, D.; Wang, H. Decreasing the spectral radius of a graph by link removals. *Phys. Rev. E* **2011**, *84*, 016101. [CrossRef] [PubMed]
20. Saha, S.; Adiga, A.; Prakash, B.A.; Vullikanti, A.K.S. Approximation algorithms for reducing the spectral radius to control epidemic spread. In Proceedings of the 2015 SIAM International Conference on Data Mining, Vancouver, BC, Canada, 30 April–2 May 2015; pp. 568–576.
21. Chakrabarti, D.; Wang, Y.; Wang, C.; Leskovec, J.; Faloutsos, C. Epidemic thresholds in real networks. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2008**, *10*, 1–26. [CrossRef]
22. Godsil, C.; Royle, G.F. *Algebraic Graph Theory*; Springer Science & Business Media: Berlin, Germany, 2013; Volume 207.
23. Cvetkovic, D.; Simic, S.; Rowlinson, P. *An Introduction to the Theory of Graph Spectra*; Cambridge University Press: Cambridge, UK, 2009.
24. ERDdS, P.; R&wi, A. On random graphs i. *Publ. Math. Debrecen* **1959**, *6*, 18.
25. Opsahl, T.; Panzarasa, P. Clustering in weighted networks. *Soc. Netw.* **2009**, *31*, 155–163. [CrossRef]
26. Kayes, A.; Han, J.; Colman, A.; Islam, M.S. RelBOSS: A relationship-aware access control framework for software services. In *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*; Springer: Berlin, Germany, 2014; pp. 258–276.
27. Kayes, A.; Rahayu, W.; Watters, P.; Alazab, M.; Dillon, T.; Chang, E. Achieving security scalability and flexibility using Fog-Based Context-Aware Access Control. *Future Gener. Comput. Syst.* **2020**, *107*, 307–323. [CrossRef]