Optimal Resource Allocation and Feasible Hexagonal Topology for Cyber-Physical Systems*

LIU Yifa · CHENG Long

DOI: 10.1007/s11424-023-2256-z
Received: 9 June 2022 / Revised: 24 July 2022

Abstract Networked cyber-physical systems are facing serious security threats from malicious attacks. It is noted that the networked cyber-physical system should take defense measures into account at the beginning of its construction. From the conservative defensive perspective, this paper proposes a robust optimal defense resource allocation strategy to reduce the maximum possible losses of the networked cyber-physical system caused by potential attacks. Then, based on the robust optimal allocation strategy, it can be proved that the topology of the networked cyber-physical system has a great influence on the loss function. In order to further improve security, the effects of adding redundant connections are investigated. Furthermore, by taking geographical knowledge into account, a hexagonal construction scheme is proposed for providing a geographically-feasible and economically-viable solution for building networked cyber-physical systems, where the loss function has a cubic decay.

Keywords Cyber-physical system, hexagonal city planning, optimization, resource allocation.

1 Introduction

In recent years, modern control systems have become more and more networked and complex[1]. Especially under the condition that integrating modern sensing, communication, and control technology is possible, the scale of networked cyber-physical systems (NCPSs) is rapidly expanding and internal interactions are more convenient and frequent[2].

The coordination between physical and cyber resources yields unprecedented capabilities, therefore, NCPSs have a wide range of applications in many fields, such as water supply[3], power systems[4, 5], transportation[6], and so on. It is noted that many NCPSs show typical hierarchical characteristics[7], for example, wastewater is pooled from all over the place to the sewage plant; the power plant provides electricity to the surrounding areas through a series of

LIU Yifa · CHENG Long (Corresponding author)
State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, *China; School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing* 100049, *China.* Email: long.cheng@ia.ac.cn.

*This research was supported by the National Natural Science Foundation of China under Grant Nos. 62025307 and U1913209.

◇ *This paper was recommended for publication by Editor Qi Hongsheng.*

facilities; and important materials like vaccines are transported to the local supply center from the producer.

However, while improving efficiency, NCPSs have also been proved to be vulnerable[8, 9], especially in the presence of various kinds of attacks including Stuxnet worm[10], false data injection (FDI) attacks[11, 12], denial of service (DoS) attacks[13], and so on. On the one hand, the combination of cyber parts and physical parts results in the duality of nodes. The node directly participates in the physical process in reality, which means that cyber attacks can directly sabotage high-value physical devices and cause a greater scale of damage than before. On the other hand, facing increasing network complexity, reliability and maintainability are difficult to be guaranteed, and there are too many nodes to be protected. Therefore, allocating limited or even insufficient defense resources to deal with malicious attacks has become a serious challenge[14].

1.1 Related Works

In the literature on the defense resource allocation of NCPSs, most investigations are based on game theory. A mean field game based method is proposed to deal with the problem of the attack-defense resource allocation for distributed nodes in mobile Ad hoc networks, where nodes lack unified planning and this problem eventually leads to a mixed strategy[15]. A game theoretical method is proposed to allocate the detection resources to adjust the detection threshold for the collaborative security detection problem based on the importance of different nodes in [16], and this classic game theoretical method requires perfect information. In [17], the communication architecture of the power grid is assumed to be tree-like, and a game based method is used to analyze the defense strategy that the defender should set encryption levels for nodes and the attack strategy that the attacker sets aggregation levels for nodes. A game theory based analysis of the DoS attacks against the remote state estimation in cyber-physical systems is presented in [18], where the attacker and the defender choose respective strategies to jam the communication channel or to send the data packet at the right time. Resource allocation for secure communications in wireless powered communication networks is studied in [19, 20], where it needs to allocate the right ratio of resources to send jamming signals against the eavesdroppers and other resources for information exchange to maximize the confidential data rate. However, in this secure communication resource allocation problem, the attacker (eavesdropper) does not need to make the decision and there is only one node considered, which results in the unique optimal solution. Fuzzy games are used to solve the problem of the attack-defense resource allocation in the vehicular network in [21], however, the final result is still a mixed strategy.

The main reasons why the existing studies cannot be directly applied to security issues of NCPSs are:

1) Many studies adopt the game theory with perfect information[15–18, 21]. Perfect information is that all players know the game structure and the payoff functions, and can instantaneously acquire the previous actions of other players. However, the defender does not know the time and location of the attack, as a result, security issues of NCPSs should be considered at the

beginning of their construction. This makes perfect information inaccessible to the defender.

2) Nash equilibrium, which is used in almost all game theoretical approaches, usually leads to mixed strategies[15, 18, 21]. However, the defender cannot timely redeploy physical defense resources to make the strategy adjustment.

1.2 Contributions

Provided the limitations of existing studies, this paper attempts to solve the problem of robust defense resource allocation in NCPSs from the following perspectives:

1) The defense resource allocation strategy should be robust. The deployment of the defense strategy precedes the attack strategy, and the defender does not know the time and other information of the attack while the attacker has enough time for reconnaissance before launching the attack against the NCPS, which makes mixed strategies not suitable. Therefore, the defender tends to prevent the worst-case scenario.

2) The defense resource allocation strategy should be analyzed in conjunction with the structure of the NCPS. Then, this paper borrows the distribution of real-world settlements and designs a feasible network structure based on geographical knowledge to further reduce the potential damage caused by attacks.

In this paper, NCPS and its vulnerable sections are modeled as a digraph and the nodes, respectively. The loss function is defined as the sum of the values of end-users who cannot get service from the center because of the attacks. An assumption that the attack resources required to cause considerable damage are far lower than the cost of the NCPS construction is adopted, which is consistent with reality observations that attack security incidents are few and attacks do not require high costs. Under this assumption, a proportional node destroying model is proposed to analyze the functional impact caused by various attack-defense resource allocations. Due to a lack of information about the potential attacks, the defender is believed to take a conservative posture. Then, the robust optimal defense resource allocation can be derived by solving a min-max problem.

Furthermore, with more attack resources applied, the probability of the case in which more than one node is destroyed simultaneously is not negligible, then the interaction between nodes should be considered and the loss function should be modified. If the upstream node has already been destroyed, all its downstream nodes cannot work in this case, and then it is not profitable to attack downstream nodes. In this situation, it can be found that the topology heavily influences the loss function.

In order to further reduce the loss function of NCPSs, the impact of topology is considered. Redundancy can reduce the loss function when upstream nodes are destroyed. Adding redundant connections is not mutually exclusive with many specific defense methods and they can be utilized simultaneously. Furthermore, considering the construction feasibility of NCPSs, a hexagonal city planning topology construction scheme based on geography is developed to provide a novel NCPS construction solution, where the loss function has a cubic decay while the number of extra redundant connections has only a double increase compared to that under the typical tree topology.

Finally, the contributions of this paper are stated as follows:

1) A loss function model of the NCPS based on the attack-defense resource allocation is proposed. By solving a min-max problem, some optimal attack-defense resource allocation strategies have been obtained under several problem settings.

2) A topological method is proposed to further reduce the loss function. The effects of adding redundant connections have been investigated.

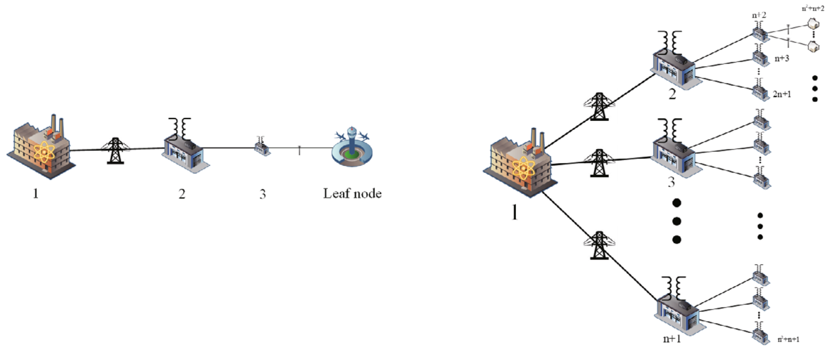
3) Hexagonal city planning based topology construction is studied to provide a geographically-feasible and cost-affordable solution for the proposed topological method.

This paper is an extension of the previously published conference paper [22], and the main differences and improvements in this paper are: This paper explains the rationality of the assumptions and gives rigorous mathematical proofs of the theorems in more detail. This paper investigates some common cases of adding redundant connections and compares them with the proposed method to demonstrate the cost performance of the proposed method.

2 Optimal Resource Allocation Strategies

2.1 Structure of NCPS

NCPSs have to deal with the actual physical process, which requires a series of facilities that are connected in functional order. Therefore, NCPS and its vulnerable sections are described by a digraph topology and nodes, respectively. For example, the water supply includes water intake, water delivery, water quality treatment, and water distribution. The facilities corresponding to each mission are different, and damage to any section can block the entire process resulting in the fact that end-users cannot receive service. Therefore, the structure of NCPS contains heterogeneous nodes, while nodes of the same level are homogeneous because they belong to the same kind of facilities. For ease of understanding, the illustration in this paper takes the power system as an example. Figure 1 shows the structure of a 4-level power grid including generation, transformation, dispatch, and end-user consumption, which is a typical case of NCPS. The notions used in this paper are defined in Table 1.



(a) (b)

Figure 1 Networked cyber-physical systems with typical topologies: (a) The line topology; (b) the perfect n-ary tree topology

Table 1 Notations

The objective is to find optimal defense strategy s_d^* to minimize loss function $L(s_a, s_d^*)$. $\mathsf{s}_{\mathsf{d}\,i}, \mathsf{s}_{\mathsf{d}}, \mathfrak{s}_{\mathfrak{d}\,ij}, \mathfrak{s}_{\mathfrak{d}\,i}$ are different elements of s_d.

Q	The total number of nodes in the NCPS topology.
$\lvert\mathcal{E}\rvert$	The number of edges in the NCPS topology.
M	The number of levels in the NCPS topology, namely the types of different facilities in the NCPS, $M > 1$.
v_{user}	The value of an end-user, namely the loss that an end-user cannot get service. All end-users have the same value.
Q_i	The number of nodes on the i-th level, $Q = \sum_{i=1}^{M} Q_i$.
p_i	The probability of node i being destroyed.
v_i	The local loss function caused by node i stopping working.
a_i, d_i	The amount of attack and defense resources allocated to node i, respectively, $A = \sum_{i=1}^{Q} a_i, 0 \leq a_i \leq A$, $D = \sum_{i=1}^{Q} d_i, A < d_i < D$.
A, D	The total amount of attack and defense resources of the attacker and the defender, respectively.
$\mathcal{U}_i$	The set of upstream nodes of node i.
s_a, s_d	The attack and defense strategies to allocate resources to each node, respectively, $s_a = [a_1\, a_2\, \cdots\, a_Q]^{\mathrm{T}}$, $s_d = [d_1\, d_2\, \cdots\, d_Q]^{\mathrm{T}}$.
$L(s_a, s_d)$	The loss function under strategies s_a and s_d.
a_{ij}, d_{ij}	The amount of attack and defense resources allocated to the j-th node on the i-th level, respectively, $\mathsf{a}_{ij} = a_{\sum_{k=1}^{i-1} Q_k + j}$, $\mathsf{d}_{ij} = d_{\sum_{k=1}^{i-1} Q_k + j}$.
$\mathsf{s}_{\mathsf{a}\,i}$, $\mathsf{s}_{\mathsf{d}\,i}$	The attack and defense strategies to allocate resources to each node on the i-th level, respectively, $\mathsf{s}_{\mathsf{a}\,i} = [\mathsf{a}_{i1}\, \cdots\, \mathsf{a}_{iQ_i}]^{\mathrm{T}}$, $s_a = [\mathsf{s}_{\mathsf{a}}{}_1^{\mathrm{T}}\, \cdots\, \mathsf{s}_{\mathsf{a}}{}_M^{\mathrm{T}}]^{\mathrm{T}}$, $\mathsf{s}_{\mathsf{d}\,i} = [\mathsf{d}_{i1}\, \cdots\, \mathsf{d}_{iQ_i}]^{\mathrm{T}}$, $s_d = [\mathsf{s}_{\mathsf{d}}{}_1^{\mathrm{T}}\, \cdots\, \mathsf{s}_{\mathsf{d}}{}_M^{\mathrm{T}}]^{\mathrm{T}}$.
v_i	The local loss function caused by the node on the i-th level stopping working.
a_i, d_i	The amount of attack and defense resources allocated to the i-th level, respectively, $\mathsf{a}_i = \sum_{j=1}^{Q_i} \mathsf{a}_{ij}, \sum_{i=1}^{M} \mathsf{a}_i = A$, $\mathsf{d}_i = \sum_{j=1}^{Q_i} \mathsf{d}_{ij}, \sum_{i=1}^{M} \mathsf{d}_i = D$.
s_{a}, s_{d}	The attack and defense strategies to allocate resources to each level, respectively, $\mathsf{s}_{\mathsf{a}} = [\mathsf{a}_1\, \mathsf{a}_2\, \cdots\, \mathsf{a}_M]^{\mathrm{T}}$, $\mathsf{s}_{\mathsf{d}} = [\mathsf{d}_1\, \mathsf{d}_2\, \cdots\, \mathsf{d}_M]^{\mathrm{T}}$.
$\mathfrak{p}_{ijk}$	The probability of the k-th node in the j-th ring on the i-th level stopping working.
$\mathfrak{a}_{ijk}$, $\mathfrak{d}_{ijk}$	The amount of attack and defense resources allocated to the k-th node in the j-th ring on the i-th level, respectively, $\mathfrak{a}_{ijk} = a_{(6^i-1)/5+6j+k}$, $\mathfrak{d}_{ijk} = d_{(6^i-1)/5+6j+k}$.
$\mathfrak{s}_{\mathfrak{a}\,ij}$, $\mathfrak{s}_{\mathfrak{d}\,ij}$	The attack and defense strategies to allocate resources to each node in the j-th ring on the i-th level, respectively, $\mathfrak{s}_{\mathfrak{a}\,ij} = [\mathfrak{a}_{ij1}\, \mathfrak{a}_{ij2}\, \cdots\, \mathfrak{a}_{ij6}]^{\mathrm{T}}$, $\mathfrak{s}_{\mathfrak{d}\,ij} = [\mathfrak{d}_{ij1}\, \mathfrak{d}_{ij2}\, \cdots\, \mathfrak{d}_{ij6}]^{\mathrm{T}}$.
$\mathfrak{L}_{ij}$	The local loss function of the j-th ring on the i-th level under strategies $\mathfrak{s}_{\mathfrak{a}\,ij}$ and $\mathfrak{s}_{\mathfrak{d}\,ij}$, if the other parts are intact.
$\mathfrak{a}_{ij}$, $\mathfrak{d}_{ij}$	The amount of attack and defense resources allocated to the j-th ring on the i-th level, respectively, $\mathfrak{a}_{ij} = \sum_{k=1}^{6} \mathfrak{a}_{ijk}$, $\mathfrak{d}_{ij} = \sum_{k=1}^{6} \mathfrak{d}_{ijk}$.
$\mathfrak{s}_{\mathfrak{a}\,i}$, $\mathfrak{s}_{\mathfrak{d}\,i}$	The attack and defense strategies to allocate resources to each ring on the i-th level, respectively, $\mathfrak{s}_{\mathfrak{a}\,i} = [\mathfrak{a}_{i1}\, \mathfrak{a}_{i2}\, \cdots\, \mathfrak{a}_{i6^{i-2}}]^{\mathrm{T}}$, $\mathfrak{s}_{\mathfrak{d}\,i} = [\mathfrak{d}_{i1}\, \mathfrak{d}_{i2}\, \cdots\, \mathfrak{d}_{i6^{i-2}}]^{\mathrm{T}}$.
$\mathfrak{L}_i$	The local loss function of the i-th level under strategies $\mathfrak{s}_{\mathfrak{a}\,i}$ and $\mathfrak{s}_{\mathfrak{d}\,i}$, if the other parts are intact.
ε	A sufficiently small positive scalar, $\varepsilon > 0$.
$\mathbf{1}_{i\times j}$	The $i \times j$ dimension matrix with all ones.
$\mathbf{1}_i$	The i dimension vector with all ones.
$\boldsymbol{e}_{ij}$	The i-th column of the $j \times j$ identity matrix, $1 \leq i \leq j$.

- Root: Generally speaking, the root is the node without a parent in a graph topology. In the NCPS, the root usually represents the service source.
- Leaf: A node with no children. The end-users are leaf nodes.
- Level: The root node is on the first level. The nodes on the i-th level indicate the i-th type facilities.
- Parent: An immediate ancestor, a node from which there is a one-step flow to the concerned node.
- Child: An immediate descendant, the converse notion of parent.
- Sibling nodes: Nodes on the same level under the same parent node.
- Ancestor/upstream node: A node reachable from the concerned node by repeated processes from child to parent operation.
- Descendant/downstream node: A node reachable from the concerned node by repeated processes from parent to child operation.
- Path: A sequence of edges $\{(i_1, i_2), (i_2, i_3), \cdots, (i_{k-1}, i_k)\}$ is called a directed path from node i_1 to node i_k. The direction from the root to the end-user is selected as the positive direction.
- Loss function: The loss function is defined as the total value of end-users who cannot get the service from the root. When the attacker launches the attack and damages the NCPS, the service supply chains of some leaf nodes are cut off and then the actual loss occurs.

2.2 Risk Function

Assumption A1 Attack resources are quite fewer than defense resources.

In the process of attacking and defending the NCPS, a series of means that both sides can take are quantified as their respective resources, and then both sides need to reasonably allocate their limited resources to achieve their goals. Attack resources include but are not limited to personnel or hackers employed to execute the malicious actions, advanced tools or malware for launching the attack, and other economic resources. And defense resources include but are not limited to staff to maintain and operate the NCPS, security tools or software, fix packs, and other economic resources. For example, for DoS attacks against event-triggered communication, the available attack duration or hashrate (computing power) that the attacker can block the communication channel is the attack resource, and additional communication resources beyond minimum requirements are the defense resources. If the attacker can block the communication so as to bring delays to the system response, the control center may make wrong decisions or the actuator may lose control to deliver unexpected performance, resulting in the service supply being affected.

The cost of building and running an NCPS is far greater than destroying it. It should be soberly aware that a single attack costing thousands has the possibility to threaten an NCPS worth billions. From another perspective, though there have been many serious accidents alerting humans to the significance of NCPS security, accidents are rare compared with most NCPSs working properly. It seems that the situation of attacks on the NCPS has not yet become extremely difficult to be dealt with. A reasonable explanation is that the attack resources are few while various security measures have been adopted.

Due to the law of diminishing marginal utility, with the more defense resources already allocated, adding extra defense resources produces fewer effects. By Assumption A1, the attack resources allocated to a single node are so small that adding more attack resources does not reduce the value of the unit resource. Therefore, the attack effect can be regarded as a linear function of quantity. Then, the probability of node i being crashed is modeled by

$$p_i = \frac{a_i}{d_i}. \tag{1}$$

Remark 2.1 The attacks discussed in this paper only affect the area where they occur, which means that the methods proposed in this paper are mainly applicable to the DoS-type attacks. And the analysis is not suitable for the attacks triggering chain reactions, like computer viruses.

2.3 Inheritance Relationship

Assumption A2 Nodes are uncorrelated to each other.

When nodes are destroyed, local loss functions are caused. If the probability of any node being destroyed is sufficiently low, the loss function is approximated as the sum of the expected local loss function of each node,

$$\mathbb{E}(L(s_a, s_d)) = \sum_{k=1}^{Q} p_k v_k = \sum_{k=1}^{Q} \frac{a_k}{d_k} v_k. \tag{2}$$

It is noted that Assumption A2 only holds in the case where the destroying probability of each node is so low that the probability of more than two nodes being damaged at the same time can be ignored. This case is also common in error detection in computer science and reliability analysis.

It is noted that the improved assumption and corresponding loss model are discussed in Section 3 where the interactions between nodes and the effect of topology on the loss function are considered.

2.4 Objective

Assumption A3 The defender should adopt conservative strategies.

The goal of the defender is to take the optimal defense resource allocation strategy to minimize the loss function, while the attacker is to choose the optimal attack resource allocation strategy for maximizing the loss function.

The optimal strategy is usually associated with game theory and many studies on defense resource allocation use game theory to simulate attack-defense scenarios. However, those optimal solutions based on game theory may not be fully applicable to the NCPS. The main reasons are:

1) NCPS security issues should be considered at the beginning of or before its construction, and defense strategies should be optimized before attacks occur. This fact makes the game theory based approach (treating attackers and defenders in an equal position) unsuitable.

2) Perfect information is that all players know the game structure and the payoff functions and can instantaneously acquire the previous actions of other players. Perfect information is widely required in game theory based approaches. In the confrontation of NCPS, the asymmetrical information puts the defender at a disadvantage position. The attacker can perform adequate reconnaissance and choose the right time before launching the attack while the defender does not know the time and location of the attack occurrence. This fact makes the game theory based methods which require the perfect information unsuitable.

3) The confrontation on NCPS is usually not dynamic. The duration of the attack may be very short when an attack occurs and there is no attack most of the time. These facts lead to that the defender may not or cannot make timely adjustments before the end of the attack. Therefore, the game theory based methods which take multiple rounds to reach Nash equilibrium are not suitable.

Due to the aforementioned analysis, once the defense strategy is deployed, the defender may not dynamically adjust the defense strategy. Then, the defender can only prevent the worst case while the attacker can achieve the best damage based on the established defense strategy. Therefore, the defender should make proper arrangements for defense resources before the attacks to reduce the maximum possible loss function. To conclude, the defender would adopt the following robust strategy,

$$\begin{aligned} s_d^* &= \operatorname*{argmin}_{s_d} \max_{s_a} \mathbb{E}(L(s_a, s_d)) = \operatorname*{argmin}_{s_d} \max_{s_a} \sum_{i=1}^{Q} \frac{a_i}{d_i} v_i, \\ s_a^* &= \operatorname*{argmax}_{s_a} \mathbb{E}(L(s_a, s_d^*)). \end{aligned}$$

Then, the loss function under the optimal strategies of both sides is

$$\mathbb{E}(L(s_a^*, s_d^*)) = \min_{s_d} \max_{s_a} \sum_{i=1}^{Q} \frac{a_i}{d_i} v_i = \sum_{i=1}^{Q} \frac{a_i^*}{d_i^*} v_i.$$

2.5 Optimal Strategy

According to [22], the difference between any two defense strategies can be formulated by the sum of aciculate variations $E_{ij} = \varepsilon(\boldsymbol{e}_{iQ} - \boldsymbol{e}_{jQ}),\ i \neq j$.

First the restrictions of resources allocated to nodes are relaxed to $\mathbb{R}^+$. Since s_a^* and s_d^* are optimal, i.e., $\mathbb{E}(L(s_a^*, s_d^*)) \geq \mathbb{E}(L(s_a^* + \Delta_{ij}, s_d^*))$, $\mathbb{E}(L(s_a^*, s_d^*)) \geq \mathbb{E}(L(s_a^* - \Delta_{ij}, s_d^*)), \forall i, j, i \neq j$, the following condition can be derived

$$\varepsilon v_i / d_i^* - \varepsilon v_j / d_j^* \leq 0, \quad -\varepsilon v_i / d_i^* + \varepsilon v_j / d_j^* \leq 0.$$

Therefore, $\varepsilon v_i / d_i^* - \varepsilon v_j / d_j^* = 0$, and this conclusion can be verified to hold under restrictions $0 \leq a_i \leq A$ and $A < d_i < D$ as well. Therefore, the optimal defense resource allocation strategy satisfies the following condition

$$\frac{d_i^*}{v_i} = \frac{d_j^*}{v_j}, \quad d_i^* = \frac{v_i}{\sum_{k=1}^{Q} v_k} D.$$

It can be seen that the defense resource allocation should be proportional to the value of the node. And the corresponding loss function can be calculated as follows

$$\mathbb{E}(L(s_a^*, s_d^*)) = \frac{A}{D} \sum_{k=1}^{Q} v_k. \tag{3}$$

The optimal attack resource allocation strategy s_a^* can be any solution satisfying the basic restriction, i.e., $\forall a_i \in [0, A]$. Therefore, optimal defense strategy s_d^* is sufficiently robust to handle any feasible attack strategies.

2.6 Evaluation of Node's Value

This subsection determines the value of the node. Since the service supply chain demands a series of different facilities, and the destruction of any facility can cut off the supply chain, the value of the i-th node v_i is equivalent to the sum of its leaves' values. The following two typical topologies are first investigated. It is noted that any directed acyclic graph can be divided into lines and trees.

2.6.1 Line

In this case, Q nodes are in series as shown in Figure 1(a). Any node being destroyed cuts off the line, and then the leaf node fails. Therefore, $v_1 = v_2 = \cdots = v_Q = v_{\text{user}}$.

Hence the attacker should focus on the most fragile node while the defense resources should be evenly distributed to all nodes, i.e., $d_i^* = D/Q, i = 1, 2, \cdots, Q$. The robust optimal defense strategy and the corresponding loss function are derived as follows:

$$s_d^* = \frac{D}{Q} \mathbf{1}_Q, \tag{4}$$

$$\mathbb{E}(L(s_a^*, s_d^*)) = \frac{A}{D} Q v_{\text{user}}. \tag{5}$$

2.6.2 Perfect n-Ary Tree

In reality, the NCPS distributes services to end-users in an area and there are many levels in NCPS. This observation makes the radial structure reasonable, especially the tree topology. Consider a perfect n-ary tree with M levels shown in Figure 1(b). It can be obtained that $\mathsf{v}_i = n^{M-i} v_{\text{user}}$. Since $Q_i = n^{i-1}$, each level has the same total value $n^{M-1} v_{\text{user}}$. Therefore, the defense resources should be evenly distributed to each level,

$$\mathsf{d}_i^* = \frac{D}{M}, \quad i = 1, 2, \cdots, M, \quad \mathsf{s}_\mathsf{d}^* = \frac{D}{M} \mathbf{1}_M.$$

And the optimal amount of defense resources allocated to the j-th node on the i-th level is given as follows

$$\mathsf{d}_{ij}^* = \frac{D}{Mn^{i-1}}, \quad j = 1, 2, \cdots, n^{i-1}, \quad \mathsf{s}_{\mathsf{d}i}^* = \frac{D}{Mn^{i-1}} \mathbf{1}_{n^{i-1}}. \tag{6}$$

The corresponding loss function can be obtained that

$$\mathbb{E}(L(s_a^*, s_d^*)) = Mn^{M-1}\frac{A}{D}v_{\text{user}}. \tag{7}$$

3 Improved Loss Function and Corresponding Allocation Strategies

Assumption A4 Nodes are relevant to each other.

Assumption A2 ignores the relationship between any two nodes. However, if there is more than one node to be destroyed, Assumption A2 may be invalid.

If the parent node can be certainly destroyed, the attacker does not need to attack the child node. The destroyed node's value can be added to the loss function only when all upstream nodes are not destroyed. Therefore, under Assumption A4, the loss function can be improved as

$$\mathbb{E}(L(s_a, s_d)) = \sum_{k=1}^{Q}\left[p_k v_k \prod_{j\in\mathcal{U}_k}(1-p_j)\right] = \sum_{k=1}^{Q}\left[\frac{a_k}{d_k}v_k \prod_{j\in\mathcal{U}_k}\left(1-\frac{a_j}{d_j}\right)\right]. \tag{8}$$

By improved loss function (8), with more attack resources deployed to the upstream node, it is less profitable to attack downstream nodes.

Remark 3.1 It is noted that (2) is always not less than (8) under the same resource allocation. Improved loss function (8) degenerates into (2) if there is no path between any two attacked nodes.

3.1 Line

According to (8), the improved loss function for the line topology can be expressed as follows

$$\frac{\mathbb{E}(L(s_a, s_d))}{v_{\text{user}}} = p_1 + p_2(1-p_1) + \cdots + p_Q\prod_{j=1}^{Q-1}(1-p_j) = 1 - \prod_{k=1}^{Q}(1-p_k). \tag{9}$$

In the line topology, because all nodes are critical, every node is a potential attack target.

Theorem 3.1 *In the line topology, the optimal defense strategy is to evenly distribute defense resources to all nodes* (*levels*)*, while the attacker should allocate all attack resources to any one node* (*level*)*, i.e.,*

$$s_a^* = \{A\boldsymbol{e}_{iQ},\ i = 1, 2, \cdots, Q\}, \quad s_d^* = \frac{D}{Q}\mathbf{1}_Q, \tag{10}$$

and the corresponding loss function is

$$\mathbb{E}(L(s_a^*, s_d^*)) = \frac{A}{D}Qv_{\text{user}}. \tag{11}$$

Proof See the proof of Theorem 3.1 in Appendix A. ∎

3.2 Perfect n-Ary Tree

Theorem 3.2 *In the perfect n-ary tree topology, the optimal defense strategy is to evenly distribute the defense resources to all levels, i.e.,*

$$\mathsf{d}_{ij}^* = \frac{D}{Mn^{i-1}}, \quad j = 1, 2, \cdots, n^{i-1}, \quad \mathsf{s}_{\mathsf{d}\,i}^* = \frac{D}{Mn^{i-1}}\mathbf{1}_{n^{i-1}},$$

while the optimal attack strategies are those avoiding the existence of paths between the attacked nodes, and the corresponding loss function is

$$\mathbb{E}(L(s_a^*, s_d^*)) = \frac{A}{D}Mn^{M-1}v_{\text{user}}. \tag{12}$$

Proof See the proof of Theorem 3.2 in Appendix B. ▌

4 Topological Method for Reducing Losses

According to (8), the loss function depends not only on the resource allocation of both sides, but also on the structure of NCPSs. If the topology can be properly modified, the robustness of the NCPS in regard to the attack can be improved. Therefore, this section makes an effort on modifying the connection topology to further reduce the loss function.

In the typical radial structure, including line and tree topology, if any node is destroyed, the leaf fails and the functionality of the NCPS is affected. As shown in Figure 2, the node can reach the root from another way if backup paths exist. Even if any non-root node is destroyed, the service can still be provided from the root to end-users[23].

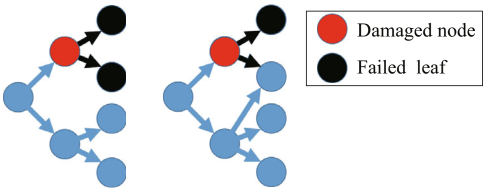


Figure 2 Node failure situations without and with redundant connections

To reduce the loss function as much as possible, an intuitive method is to add a sufficient number of connections. And doing so can definitely achieve desired results. In this section, an extreme case is studied. That is: Every node is connected to all nodes on the previous level as shown in Figure 3.

Consider an NCPS with M levels and the total value of all end-users is $Q_M v_{\text{user}}$. Under this extreme case, the only way to cause damage is to cut off all nodes on one level and the loss function is obtained as follows

$$\mathbb{E}(L(s_a, s_d)) = \left[1 - \prod_{i=1}^{M}\left(1 - \prod_{j=1}^{Q_i}\frac{\mathsf{a}_{ij}}{\mathsf{d}_{ij}}\right)\right]Q_M v_{\text{user}}.$$

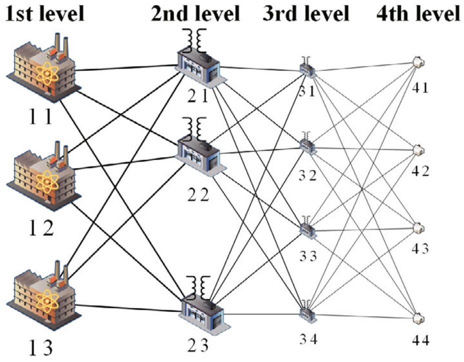


Figure 3 Fully connected NCPS: Link every facility to all its upstream and downstream facilities

The allocation of resources can be divided into the following two sub-problems.

Resource Allocation within One Level

Theorem 3.3 *In a fully connected topology, for any level, the attacker and the defender should distribute their resources evenly to each node on that level, respectively, i.e.,*

$$\mathsf{a}^*_{ij} = \frac{\mathsf{a}_i}{Q_i}, \quad \mathsf{s}^*_{\mathsf{a}\,i} = \frac{\mathsf{a}_i}{Q_i}\mathbf{1}_{Q_i}, \quad \mathsf{d}^*_{ij} = \frac{\mathsf{d}_i}{Q_i}, \quad \mathsf{s}^*_{\mathsf{d}\,i} = \frac{\mathsf{d}_i}{Q_i}\mathbf{1}_{Q_i}. \tag{13}$$

Proof See the proof of Theorem 3.3 in Appendix C. ∎

Under those strategies, the probability of the i-th level being destroyed can be calculated as follows

$$\prod_{j=1}^{Q_i} \frac{\mathsf{a}^*_{ij}}{\mathsf{d}^*_{ij}} = \prod_{j=1}^{Q_i} \frac{\mathsf{a}_i/Q_i}{\mathsf{d}_i/Q_i} = (\mathsf{a}_i/\mathsf{d}_i)^{Q_i}.$$

Resource Allocation to Different Levels

Theorem 3.4 *In a fully connected topology, the attacker should allocate all attack resources to any and only one level, while the optimal defense strategy is to distribute the defense resources in such a way that the loss function keeps invariant under all possible attack strategies, i.e.,*

$$\mathsf{s}^*_{\mathsf{a}} = \{A\boldsymbol{e}_{iM},\ i = 1, 2, \cdots, M\}, \quad \mathsf{s}^*_{\mathsf{a}\,i} = \frac{\mathsf{a}_i}{Q_i}\mathbf{1}_{Q_i}, \tag{14}$$

$$\sum_{j=1}^{M} \left(\frac{\mathsf{d}^*_i}{A}\right)^{\frac{Q_i}{Q_j}} = \frac{D}{A}, \quad i = 1, 2, \cdots, M. \tag{15}$$

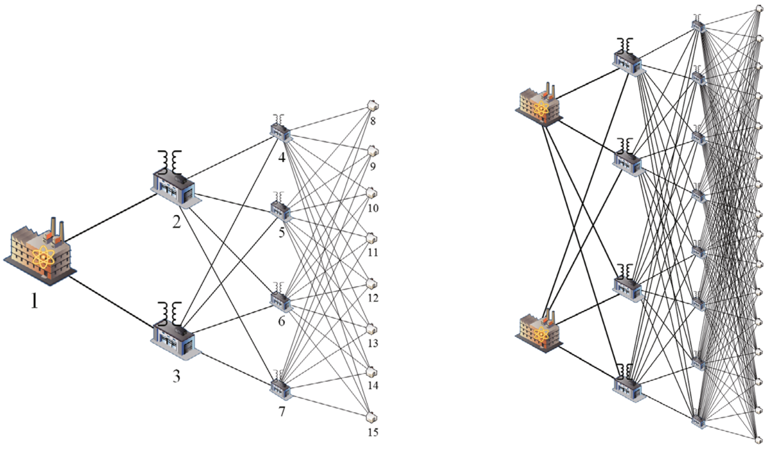
Proof See the proof of Theorem 3.4 in Appendix D. ∎

Remark 4.1 Levels with more nodes can have more redundant connections. Therefore, those levels occupy fewer defense resources by (15).

The following subsections are to give some special topologies which can lead to an approximate solution to (15), and the corresponding loss function reduction can be viewed more clearly.

4.1 Fully Connected Tree

This section studies a special topology, the perfect n-ary tree with the addition of all possible connections, which is shown in Figure 4(a). $Q_i = n^{i-1},\ i = 1, 2, \cdots, M$.



(a) (b)

Figure 4 Modified NCPS structures after adding all possible connections: (a) Fully connected tree; (b) fully connected forest

By (15), for the M-th level, d_M^* satisfies that

$$\sum_{j=1}^{M}\left(\frac{\mathsf{d}_M^*}{A}\right)^{n^{M-j}} = \frac{D}{A}. \tag{16}$$

Since $\mathsf{d}_M^* > A$ and $n \geq 2$, $(\mathsf{d}_M^*/A)^{n^{M-1}}$ is significantly greater than the other terms on the left hand, and the solution to (16) can be approximated by

$$\mathsf{d}_M^* \approx A^{1-\frac{1}{n^{M-1}}} D^{\frac{1}{n^{M-1}}}. \tag{17}$$

By substituting (17) into (32), it can be obtained that

$$\mathsf{d}_i^* \approx A^{1-\frac{1}{n^{i-1}}} D^{\frac{1}{n^{i-1}}}, \quad i = 2, 3, \cdots, M, \quad \mathsf{d}_1^* = D - \sum_{i=2}^{M} \mathsf{d}_i^* \approx D. \tag{18}$$

Therefore, under the case of the "fully connected tree", the optimal attack strategy is

$$\mathsf{s}_\mathsf{a}^* = \{A\boldsymbol{e}_{iM},\ i = 1, 2, \cdots, M\}, \quad \mathsf{s}_{\mathsf{a}i}^* = \frac{\mathsf{a}_i}{n^{i-1}}\mathbf{1}_{n^{i-1}}.$$

The approximate optimal defense strategy and the corresponding loss function are

$$\mathsf{s}_{\mathsf{d}i}^* \approx A^{1-\frac{1}{n^{i-1}}} D^{\frac{1}{n^{i-1}}} \frac{1}{n^{i-1}}\mathbf{1}_{n^{i-1}}, \tag{19}$$

$$E(L(s_a^*, s_d^*)) \approx \frac{A}{D} n^{M-1} v_{\text{user}}. \tag{20}$$

The loss function has been reduced to $1/M$ of that of (12) by adding redundant connections. As to the cost, the fully connected tree requires the following number of connections

$$|\mathcal{E}|_{\text{FC tree}} = (n^{2M-1} - n)/(n^2-1) \approx n^{2M-3} \approx n^{M-2}|\mathcal{E}|_{\text{tree}}.$$

The root in a fully connected tree is an isolated node and becomes the most fragile section. Too many resources have to be invested to defend the root (by (18), $\mathsf{d}_1^* \approx D$).

4.2 Fully Connected Forest

If there are many “roots” in an area to backup each other, the reliability of the entire networked system can be greatly improved. This subsection considers the case that there are multiple service providers or goods producers, namely the nodes on the first level.

Combining n perfect n-ary trees leads to the topology with n roots. This topology is shown in Figure 4(b). The total amounts of attack and defense resources become nA and nD, respectively. Similar to the above analysis, the optimal attack resource strategy is given as follows

$$\mathsf{s}_{\mathsf{a}}^* = \{nA\boldsymbol{e}_{iM},\ i = 1, 2, \cdots, M\}, \quad \mathsf{s}_{\mathsf{a}\,i}^* = \frac{\mathsf{a}_i}{n^{i-1}}\mathbf{1}_{n^i}. \tag{21}$$

Similarly, the approximate optimal defense strategy and the corresponding loss function are

$$\begin{aligned} \mathsf{s}_{\mathsf{d}\,i}^* &\approx A^{1-\frac{1}{n^{i-1}}} D^{\frac{1}{n^{i-1}}} \frac{1}{n^{i-1}}\mathbf{1}_{n^i}, \\ E(L(s_a^*, s_d^*)) &\approx \left(\frac{A}{D}\right)^n n^M v_{\text{user}}. \end{aligned} \tag{22}$$

By (22), the loss function can be significantly reduced compared with that of (20). However, the cost of redundant connections has reached the following unacceptable level

$$|\mathcal{E}|_{\text{FC forest}} = \frac{n^{2M+1} - n^3}{n^2 - 1} \approx n^{2M-1} \approx n^{M-1}|\mathcal{E}|_{\text{forest}}. \tag{23}$$

5 Geographical Knowledge Based NCPS Construction

Section 4 discusses the impact of different topologies on the loss function, however, the construction planning of NCPSs cannot be guided by only topology information[23]. The reasons are:

1) Topology ignores location information, which cannot describe the geographical distribution. Service should go through a series of different facilities. All facilities are physically present in reality and site selection should be considered seriously.

2) Topology ignores the capacity of the actual facility. In the previous topological analysis, to cut off a node, the attacker must destroy all of its parent nodes, which means that every node must have sufficient capacity of supplying all its child nodes. The most extreme case is that one node has the capacity for the entire system, which is unnecessary and almost impossible. Hence, the additional capacity requirements for facilities must be considered in the construction of the NCPS.

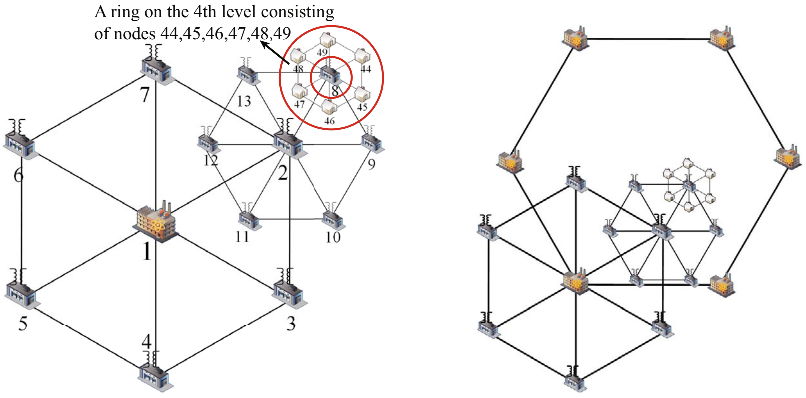
3) Edges in the topology cannot fully express the function of the service supply chain in reality. Although the facilities may be sabotaged by attacks, connections between those facilities are intact or easy to bridge. As long as there is a full set of facilities with adequate capacity on the path, the supply chain can be completed. Therefore, redundant connections can be added between nodes on the same level such that when one node is damaged, its siblings can undertake part of this node's responsibility.

This section is to develop a geographically-feasible solution for NCPS construction by considering the function, capacity, and geographical distribution of facilities.

"Central Place Theory" is a geographical theory to explain the number, size, and location of human settlements in a residential system[24]. Based on this theory, hexagonal city planning was proposed to solve the problem of providing services to surrounding areas, which is a cost-effective and efficient land use pattern in geography. Since the NCPS aims at providing services or goods to the end-users, its construction can follow the hexagonal planning principle.

5.1 Hexagonal City Group

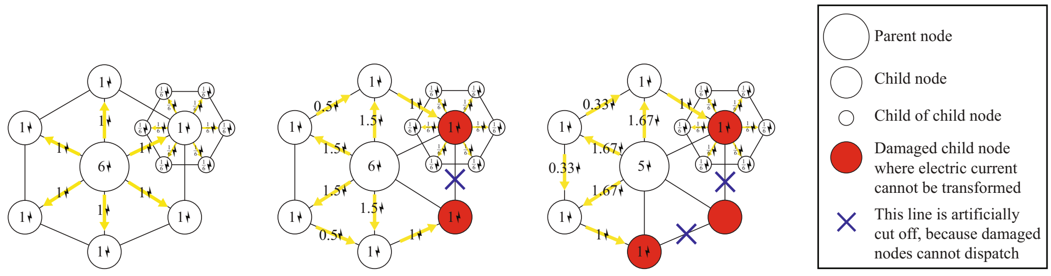
Based on the hexagonal planning principle, a geographically feasible topology construction scheme is proposed for the NCPS as shown in Figure 5(a). The main difference between this topology and a perfect 6-ary tree is that every non-root node is connected to its two adjacent siblings so that six children form a ring.


A ring on the 4th level consisting
of nodes 44,45,46,47,48,49
49
48
44
8
47
45
46
7
13
6
12
2
9
1
11
10
5
3
4

(a) (b)

Figure 5 An NCPS construction under the hexagonal city group structure: (a) Hexagonal city groups; (b) groups of six hexagonal city groups

From Figure 6, if the capacity of each facility is twice its basic demand, as long as less than three nodes are destroyed, the adjacent nodes can share the functions of the destroyed nodes, and then the normal operation of the NCPS can be maintained. At least three nodes are destroyed and the destroyed nodes are adjacent, the descendant of the middle node can be affected.


Parent node
Child node
Child of child node
Damaged child node where electric current cannot be transformed
This line is artificially cut off, because damaged nodes cannot dispatch
6
5
1
0.5
1.5
0.33
1.67

(a) (b) (c)

Figure 6 Operation conditions of NCPS under different scenarios: (a) Normal operation; (b) two nodes damaged; (c) three adjacent nodes damaged

Assume the hexagonal structure has M levels. The probability of the service cannot pass through a non-root node is approximately equivalent to the probability that this node and two adjacent siblings are destroyed, namely the probability of the k-th node in the j-th ring on the i-th level stopping working can be calculated as follows

$$\mathfrak{p}_{ijk}=\frac{\mathfrak{a}_{ij[(k+4)\bmod 6+1]}}{\mathfrak{d}_{ij[(k+4)\bmod 6+1]}}\frac{\mathfrak{a}_{ijk}}{\mathfrak{d}_{ijk}}\frac{\mathfrak{a}_{ij[k\bmod 6+1]}}{\mathfrak{d}_{ij[k\bmod 6+1]}}.$$

The local loss function caused by one node on the i-th level stopping working can be expressed as $\mathsf{v}_i=6^{M-i}v_{\text{user}}$. Because the probability of four or more nodes being simultaneously destroyed is much smaller than that of three nodes under Assumption A1, the expected loss function of the j-th ring on the i-th level $(i=2,\cdots,M;\ j=1,\cdots,6^{i-2})$ is

$$\mathbb{E}(\mathfrak{L}_{ij}(\mathfrak{s}_{\mathfrak{a}ij},\mathfrak{s}_{\mathfrak{d}ij}))=\sum_{k=1}^{6}\mathfrak{p}_{ijk}\mathsf{v}_i.$$

And then the loss function of the entire NCPS can be expressed by the sum of local loss functions of all rings as follows

$$\begin{aligned}\mathbb{E}(L(s_a,s_d))=\,&p_1\mathsf{v}_1+(1-p_1)E(\mathfrak{L}_{21})\\&+\sum_{i=1}^{6}(1-p_1)(1-\mathfrak{p}_{21i})E(\mathfrak{L}_{3i})\\&+\sum_{i=1}^{6}\sum_{j=1}^{6}(1-p_1)(1-\mathfrak{p}_{21i})(1-\mathfrak{p}_{3ij})E(\mathfrak{L}_{4[6(i-1)+j]})\\&+\cdots\\&+\sum_{i=1}^{6}\cdots\sum_{z=1}^{6}(1-p_1)(1-\mathfrak{p}_{21i})\cdots(1-\mathfrak{p}_{[M-1][6^{M-4}(i-1)+\cdots]z})\\&\quad E(\mathfrak{L}_{M[6^{M-3}(i-1)+\cdots+z]}).\end{aligned}$$

After obtaining the loss function, the optimal attack-defense resource allocation strategies can be calculated. Similar to the analysis in Section 4, the resource allocation problem can be divided into the following three sub-problems.

Resource Allocation within a Ring

Theorem 5.1 *Within any ring of the hexagonal structure, the defender and the attacker should evenly distribute their respective resources to each node on that ring, i.e.,*

$$\mathfrak{a}^*_{ijk} = \frac{\mathfrak{a}_{ij}}{6}, \quad \mathfrak{s}^*_{\mathfrak{a}ij} = \frac{\mathfrak{a}_{ij}}{6}\mathbf{1}_6, \quad \mathfrak{d}^*_{ijk} = \frac{\mathfrak{d}_{ij}}{6}, \quad \mathfrak{s}^*_{\mathfrak{d}ij} = \frac{\mathfrak{d}_{ij}}{6}\mathbf{1}_6.$$

And the corresponding local loss function of this ring is

$$\mathbb{E}(\mathfrak{L}_{ij}(\mathfrak{s}^*_{\mathfrak{a}ij}, \mathfrak{s}^*_{\mathfrak{d}ij})) = 6^{M-i+1}\left(\frac{\mathfrak{a}_{ij}}{\mathfrak{d}_{ij}}\right)^3 v_{\text{user}}.$$

Proof See the proof of Theorem 5.1 in Appendix E. ▮

Resource Allocation to Different Rings on the Same Level

Theorem 5.2 *Within any level of the hexagonal structure, the defender should distribute resources evenly to each ring on that level, while the attacker should allocate all attack resources to any and only one ring on that level, i.e.,*

$$\begin{aligned}
&\mathfrak{a}^*_{ijk} = \frac{\mathfrak{a}_{ij}}{6}, \quad \mathfrak{s}^*_{\mathfrak{a}i} = \{\mathfrak{a}_i \boldsymbol{e}_{l6^{i-2}}, l = 1, 2, \cdots, 6^{i-2}\},\\
&\mathfrak{d}^*_{ijk} = \frac{\mathsf{d}_i}{6^{i-1}}, \quad \mathfrak{s}^*_{\mathfrak{d}i} = \frac{\mathsf{d}_i}{6^{i-2}}\mathbf{1}_6^{i-2}.
\end{aligned}$$

And the local loss function of the i-th ($i > 2$) *level is*

$$\mathbb{E}(\mathfrak{L}_i(\mathfrak{s}^*_{\mathfrak{a}i}, \mathfrak{s}^*_{\mathfrak{d}i})) = 6^{M+2i-5}\left(\frac{\mathsf{a}_i}{\mathsf{d}_i}\right)^3 v_{\text{user}}. \tag{24}$$

Proof See the proof of Theorem 5.2 in Appendix F. ▮

Resource Allocation to Different Levels

Theorem 5.3 *For different levels of the hexagonal structure, the attacker should allocate all attack resources to any and only one level, while the defense resources should be distributed in such a way that the loss function keeps constant under any attack strategy, i.e.,*

$$\mathfrak{s}_{\mathfrak{a}} = \{A\mathbf{e_k},\ k = 1, 2, \cdots, M\}, \tag{25}$$

$$\begin{aligned}
6^{M-1}\frac{A}{\mathsf{d}_1}v_{\text{user}} &= 6^{M-1}\left(\frac{A}{\mathsf{d}_2}\right)^3 v_{\text{user}} = \cdots = 6^{M+2i-5}\left(\frac{A}{\mathsf{d}_i}\right)^3 v_{\text{user}}\\
&= \cdots = 6^{3M-5}\left(\frac{A}{\mathsf{d}_M}\right)^3 v_{\text{user}}.
\end{aligned} \tag{26}$$

Proof See the proof of Theorem 5.3 in Appendix G. ▮

By considering the above three cases and the fact that the total amount of defense resources is $\sum_{i=1}^{M} \mathsf{d}_i = D$, the approximate solution to (26) is

$$\mathsf{d}_1^* \approx D, \quad \mathsf{d}_i^* \approx 6^{\frac{2i-4}{3}} A^{\frac{2}{3}} D^{\frac{1}{3}}, \quad i = 2, 3, \cdots, M.$$

And the final optimal defense-attack resource allocation strategies are

$$\begin{aligned}
&\mathfrak{a}_{ijk}^* = \frac{\mathfrak{a}_{ij}^*}{6}, \quad \mathfrak{s}_{\mathfrak{a}i}^* = \{\mathsf{a}_i^* \boldsymbol{e}_{l6^{i-2}}, l = 1, 2, \cdots, 6^{i-2}\}, \quad \mathsf{s}_{\mathsf{a}}^* = \{A\boldsymbol{e}_{iM}, i = 1, 2, \cdots, M\}, \\
&d_1^* \approx D, \quad \mathfrak{d}_{ijk}^* \approx 6^{-\frac{i+1}{3}} A^{\frac{2}{3}} D^{\frac{1}{3}}, \quad i = 2, 3, \cdots, M, \\
&\mathsf{d}_1^* \approx D, \quad \mathsf{d}_i^* = 6^{\frac{2i-4}{3}} A^{\frac{2}{3}} D^{\frac{1}{3}}, \quad i = 2, 3, \cdots, M.
\end{aligned}$$

And the corresponding loss function is

$$\mathbb{E}((s_a^*, s_d^*)) \approx \frac{A}{D} 6^{M-1} v_{\text{user}}.$$

From the above discussion, it can be seen that the topology of the hexagonal city group can approximately reach the same expected loss function as the one of the fully connected tree defined by (20), while the total number of required connections is

$$|\mathcal{E}|_{\text{Hexagonal city group}} = 2(6^M - 6)/5 = 2|\mathcal{E}|_{\text{6-ary tree}},$$

which is only twice that of the classical 6-ary tree topology.

5.2 Groups of Hexagonal City Groups

Similar to Subsection 4.2, since the root node has no substitute, it becomes the most fragile section, and thus too many defense resources have to be placed on the root. If there are more nodes on the first level to form a ring as Figure 5(b), the loss function could further decrease.

Consider a group of 6 city groups, and the total amounts of the attack resources and defense resources are set to $6A$ and $6D$, respectively. In this case, the first level is made of one ring and satisfies the loss function defined by (24). By adding the local loss functions of all levels, the total loss function can be derived as follows

$$\mathbb{E}(L(s_a, s_d)) = \sum_{i=1}^{M} 6^{M+2i-5} \left(\frac{\mathsf{a}_i}{\mathsf{d}_i}\right)^3 v_{\text{user}}. \tag{27}$$

Based on (27), the optimal amount of defense resources allocated to each level satisfies the following conditions

$$6^{M-3}\left(\frac{6A}{\mathsf{d}_1^*}\right)^3 = \cdots = 6^{M+2i-5}\left(\frac{6A}{\mathsf{d}_i^*}\right)^3 = \cdots = 6^{3M-5}\left(\frac{6A}{\mathsf{d}_M^*}\right)^3.$$

Notice the fact that $\sum_{i=1}^{M} \mathsf{d}_i{}^* = 6D$, it can be solved that

$$\mathsf{d}_i^* = \frac{6^{\frac{2i}{3}} - 6^{\frac{2i-2}{3}}}{6^{\frac{2M}{3}} - 1} 6D.$$

According to Theorems 5.1, 5.2, and 5.3, to maximize the loss function, the attacker should choose any one ring on any level and evenly distribute the attack resources to each node on that ring. That is:

$$\mathfrak{a}^*_{ijk} = \frac{\mathfrak{a}^*_{ij}}{6}, \quad \mathfrak{s}^*_{\mathfrak{a}i} = \{\mathsf{a}^*_i \boldsymbol{e}_{l6^{i-1}}, l = 1, 2, \cdots, 6^{i-1}\},$$

$$\mathsf{s}^*_{\mathsf{a}} = \{6A\boldsymbol{e}_{iM}, i = 1, 2, \cdots, M\}, \quad \mathfrak{d}^*_{ijk} = \frac{6^{\frac{2i}{3}} - 6^{\frac{2i-2}{3}}}{6^{\frac{2M}{3}} - 1} \frac{1}{6^i}(6D).$$

Then, the corresponding loss function is obtained as follows

$$\mathbb{E}(L(s^*_a, s^*_d)) = 6^{M-7}\left(\frac{6^{\frac{2M}{3}} - 1}{6^{\frac{2}{3}} - 1}\right)^3 \left(\frac{A}{D}\right)^3 v_{\text{user}}. \tag{28}$$

From (28), the loss function under this complete hexagonal city planning has a "cubic-level" reduction while the required number of connections is only twice that of the forest topology,

$$|\mathcal{E}|_{\text{Group of hexagonal cities}} = 12(6^M - 6)/5 + 6 \approx 2|\mathcal{E}|_{\text{6-ary forest}}.$$

6 Numerical Studies

This section gives some numerical studies regarding the loss function under different topologies to verify the theoretical analysis.

6.1 Single Root Case

Consider a centralized NCPS (only one root node) with M levels and 6^{M-1} users in total. Each non-leaf node in the system has 6 children. The reduced loss function and required connections under different topologies are shown in Table 2. From Table 2, the loss function of the fully connected tree topology can be reduced to $1/M$ of that of the original topology, however, the number of edges required for such a structure is unacceptable. Hexagonal city group planning can achieve a loss reduction similar to the one of a fully connected tree while the number of connections is twice as high as that of the original tree topology.

Table 2 Comparison under different topologies with single root

Topology	Leaves	Edges	$E(L(s^*_a, s^*_d))$	Added Edges	Reduced Loss Function
Perfect 6-ary Tree	6^{M-1}	$\frac{6}{5}(6^{M-1}-1)$	$M6^{M-1}\frac{A}{D}v_{\text{user}}$	0	0
Fully Connected Tree	6^{M-1}	$\frac{6}{35}(6^{2M-2}-1)$	$6^{M-1}\frac{A}{D}v_{\text{user}}$	$O(6^{2M-3})$	$(M-1)6^{M-1}\frac{A}{D}v_{\text{user}}$
Hexagonal City Group	6^{M-1}	$\frac{12}{5}(6^{M-1}-1)$	$6^{M-1}\frac{A}{D}v_{\text{user}}$	$\frac{6}{5}(6^{M-1} - 1)$	$(M-1)6^{M-1}\frac{A}{D}v_{\text{user}}$

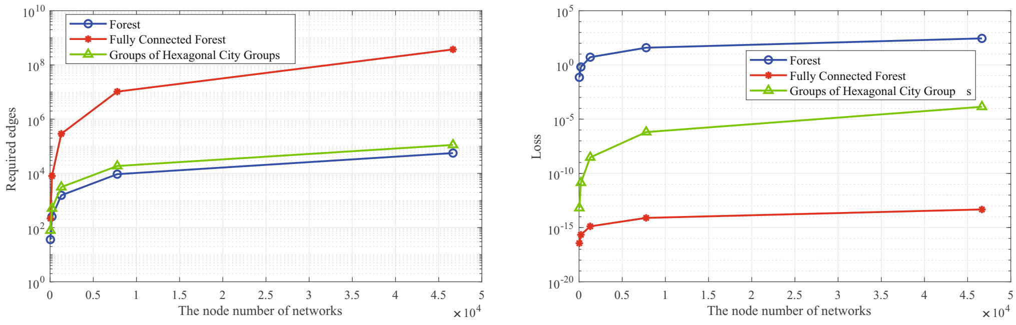
6.2 Multiple "Roots" Case

In this case, it is assumed that there are 6 NCPSs originally. Then, there are 6 root nodes and 6^M users in total. The loss functions under different topologies are discussed in Table 3. From this table, the hexagonal city group topology obtains a better performance at an affordable cost. The loss function has a cubic-level decay.

In the experiment, the value of each end-user is set to 1, and the total attack and defense resources are set to 60 and 60000, respectively. Figure 7 shows the results of the configuration on three types of NCPS topologies.

Table 3 Comparison of different topologies with six "roots"

Topology	Leaves	Edges	$E(L(s_a^*, s_d^*))$	Added Edges
Forest	6^M	$\frac{6}{5}(6^M-6)$	$M6^M\frac{A}{D}v_{\text{user}}$	0
Fully Connected Forest	6^M	$\frac{216}{35}(6^{2M-2}-1)$	$6^M(\frac{A}{D})^6 v_{\text{user}}$	$O(6^{2M-1})$
Groups of Hexagonal City Groups	6^M	$\frac{12}{5}(6^M-6)+6$	$6^{M-7}(\frac{6^{\frac{2M}{3}}-1}{6^{\frac{2}{3}}-1})^3(\frac{A}{D})^3 v_{\text{user}}$	$\frac{6}{5}(6^M-6)+6$



(a) (b)

Figure 7 Performance comparison of different topologies: (a) Edge number; (b) loss function

In particular, let the power grid as a typical NCPS. Assume each power grid has 5 levels (power plant, step-up, primary step-down, secondary step-down, distribution station), and the total value of all users is 7776. Then, under the original topology (6 independent 6-ary trees), there are 9324 edges, and the expected loss function is 38.88. Under the fully connected forest topology, the expected loss function is 7.776×10^{-15}, however, the number of added edges is 10356300 and each facility should have the capacity of supporting the entire grid. Under the hexagonal city planning, the expected loss function is 1.3665×10^{-4} while the number of added edges is only 9330 and the capacity of each facility is only required to be twice the basic demand.

To summarize, the hexagonal city planning scheme developed in this paper does not have to add too many additional connections, while this scheme can reduce the loss function effectively. It can improve not only the security of the NCPS but also the efficiency of infrastructure investment in the NCPS.

7 Conclusion

The operation of the NCPS requires the coordination of various facilities, and the failure of any section or facility can cut off the service supply. Therefore, concentrated attacks can create better destructive effects. Inversely, the defender has to guarantee the security of every facility. Redundancy can help to maintain the normal operation of the NCPS by utilizing the assistance of other facilities after some facilities are destroyed.

When it comes to redundant connections, feasibility, price, and capacity should be taken into consideration. To this end, this paper develops a hexagonal city planning scheme. In this scheme, any vulnerable section has a "backup" in an emergency. By taking this approach, the loss function of the networked system has a cubic-level decay while the number of edges and the capacities of facilities are only required to be twice those used in the classical system with the tree topology. In addition, the hexagonal city planning theory is based on the settlements' physical distribution. Therefore, the proposed method for the NCPS is highly geographically-feasible.

References

[1] Liu GP, Networked learning predictive control of nonlinear cyber-physical systems, *Journal of Systems Science and Complexity*, 2020, **33**(6): 1719–1732.

[2] Sha L, Gopalakrishnan S, Liu X, et al, Cyber-physical systems: A new frontier, *Proceedings of* 2008 *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taiwan, China, 2008, 1–9.

[3] Sun C, Cembrano G, Puig V, et al, Cyber-physical systems for real-time management in the urban water cycle, *Proceedings of* 2018 *International Workshop on Cyber-Physical Systems for Smart Water Networks*, 2018, 5–8.

[4] Mo Y, Kim T H, Brancik K, et al, Cyber-physical security of a smart grid infrastructure, *Proceedings of the IEEE*, 2012, **100**(1): 195–209.

[5] Lu G, De D, and Song W, SmartGridLab: A laboratory-based smart grid testbed, *Proceedings of the First IEEE International Conference on Smart Grid Communications*, Gaithersburg, USA, 2010, 143–148.

[6] Younis O and Moayeri N, Employing cyber-physical systems: Dynamic traffic light control at road intersections, *IEEE Internet of Things Journal*, 2017, **4**(6): 2286–2296.

[7] Wang L, Lin F, and Yin G, Network robustness depth and topology management of networked dynamic systems, *Journal of Systems Science and Complexity*, 2016, **29**(1): 1–21.

[8] Wen G, Yu W, Yu X, et al, Complex cyber-physical networks: From cybersecurity to security control, *Journal of Systems Science and Complexity*, 2017, **30**(1): 46–67.

[9] Sridhar S, Hahn A, and Govindarasu M, Cyber-physical system security for the electric power grid, *Proceedings of the IEEE*, 2012, **100**(1): 210–224.

[10] Lindsay J R, Stuxnet and the limits of cyber warfare, *Security Studies*, 2013, **22**(3): 365–404.

[11] Zhang Q, Liu K, Xia Y, et al, Optimal stealthy deception attack against cyber-physical systems, *IEEE Transactions on Cybernetics*, 2020, **50**(9): 3963–3972.

[12] Zhang X, Liu Y, and Zhang Y, A secure clock synchronization scheme for wireless sensor networks against malicious attacks, *Journal of Systems Science and Complexity*, 2021, **34**(6): 2125–2138.

[13] Zhang H and Zheng W X, Denial-of-service power dispatch against linear quadratic control via a fading channel, *IEEE Transactions on Automatic Control*, 2018, **63**(9): 3032–3039.

[14] Mo H and Sansavini G, Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks, *IEEE Transactions on Reliability*, 2017, **66**(4): 1253–1265.

[15] Wang Y, Yu F R, Tang H, et al, A mean field game theoretic approach for security enhancements in mobile Ad hoc networks, *IEEE Transactions on Wireless Communications*, 2014, **13**(3): 1616–1627.

[16] Wu H and Wang W, A game theory based collaborative security detection method for internet of things systems, *IEEE Transactions on Information Forensics and Security*, 2018, **13**(6): 1432–1445.

[17] Ismail Z, Leneutre J, Bateman D, et al, A game theoretical analysis of data confidentiality attacks on smart-grid AMI, *IEEE Journal on Selected Areas in Communications*, 2014, **32**(7): 1486–1499.

[18] Li Y, Shi L, Cheng P, et al, Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach, *IEEE Transactions on Automatic Control*, 2015, **60**(10): 2831–2836.

[19] Abedi M R, Mokari N, Saeedi H, et al, Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary, *IEEE Transactions on Wireless Communications*, 2017, **16**(2): 885–899.

[20] Xu D and Li Q, Resource allocation for secure communications in cooperative cognitive wireless powered communication networks, *IEEE Systems Journal*, 2019, **13**(3): 2431–2442.

[21] Alpcan T and Buchegger S, Security games for vehicular networks, *IEEE Transactions on Mobile Computing*, 2011, **10**(2): 280–290.

[22] Liu Y and Cheng L, Optimal defense resource allocation and geographically feasible hexagonal topology construction for power grid security, *Communications in Computer and Information Science*, 2021, **1468**: 452–462.

[23] Wang H, Zhao Q, Jia Q, et al, Efficient topology optimization for a wired networked system by adding wireless communication, *Proceedings of* 2012 *American Control Conference*, Montreal, Canada, 2012, 448–453.

[24] Hsu W and Zou X, Central place theory and the power law for cities, *The Mathematics of Urban Morphology*, 2019, 55–75.

Appendix A: The Proof of Theorem 3.1

When the defender takes defense strategy (4), i.e., $d_i = D/Q$, the attacker can choose any node as the target,

$$s_a = \{A\boldsymbol{e}_{iQ},\ i = 1, 2, \cdots, Q\}. \tag{29}$$

And the loss function defined by (8) can be calculated as $E(L(s_a, s_d)) = QAv_{\text{user}}/D$, which is equal to (5). If the attacker chooses more than one node as the target, i.e., $a_i > 0$, $a_j > 0$, (9) becomes

$$\begin{aligned}
&1 - \left(1-Q\frac{a_i}{D}\right)\left(1-Q\frac{a_j}{D}\right)\prod_{k=1,k\neq i,j}^{Q}\left(1-Q\frac{a_k}{D}\right)\\
&= 1 - \left(1-Q\frac{a_i}{D}-Q\frac{a_j}{D}+Q^2\frac{a_ia_j}{D^2}\right)\prod_{k=1,k\neq i,j}^{Q}\left(1-Q\frac{a_k}{D}\right)\\
&< 1 - \left(1-Q\frac{a_i+a_j}{D}\right)\left(1-Q\frac{0}{D}\right)\prod_{k=1,k\neq i,j}^{Q}\left(1-Q\frac{a_k}{D}\right).
\end{aligned}$$

By repeating this operation, it can be concluded that the attack strategy defined by (29) can lead to greater loss function than any other attack strategy. Due to Remark 3.1, the loss function is no greater than (5). Therefore, attack strategy (29) is optimal under defense strategy (4).

If the defender takes a defense strategy other than (4), there exists a node j such that $d_j < D/Q$. Then, if all attack resources are allocated to node j, the loss function is greater than (5). Therefore, defense strategy (4) is robust optimal as well.

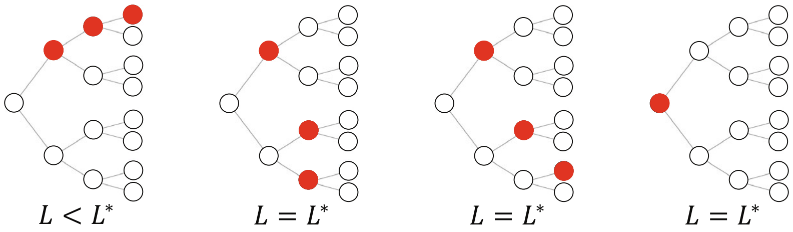
By the above analysis, under the line topology, the optimal strategies of both sides and the corresponding loss function are summarized as follows

$$s_a^* = \{A\boldsymbol{e}_{iQ},\ i = 1, 2, \cdots, Q\}, \quad s_d^* = \frac{D}{Q}\mathbf{1}_Q, \quad \mathbb{E}(L(s_a^*, s_d^*)) = \frac{A}{D}Qv_{\text{user}}.$$

Although the loss function model is changed, the attacker can centralize resources to avoid loss reduction. Conversely, the defender should take the same strategy as (4).

Appendix B: The Proof of Theorem 3.2

When the defender takes defense strategy (6), denote L as the loss function that can be achieved. Denote $L^* = Mn^{M-1}Av_{\text{user}}/D$, which is equivalent to the loss function in (7). According to Remark 3.1, $L \leq L^*$. From different attack target selections shown in Figure 8, it can be seen that the existence of a path can be always avoided by the attacker. Therefore, maximal loss function L^* can be still obtained in a tree topology. And all nodes are threatened as that in Subsection 2.6.2.



(a) (b) (c) (d)

Figure 8 Cases of target selections in a tree topology

If the defender adopts a defense strategy other than (6), there exists at least one node whose allocated defense resources are less than those in (6). If all attack resources are allocated to this node, the loss function becomes greater than (7). Therefore, defense strategy (6) is robust optimal. To conclude, the robust optimal defense strategy under the improved loss function is

$$\mathsf{d}_{ij}^* = \frac{D}{Mn^{i-1}}, \quad j = 1, 2, \cdots, n^{i-1}, \quad \mathsf{s}_{\mathsf{d}i}^* = \frac{D}{Mn^{i-1}}\mathbf{1}_{n^{i-1}}.$$

Besides, the optimal attack strategies are those having no path between the attacked nodes. And the corresponding loss function is

$$\mathbb{E}(L(s_a^*, s_d^*)) = \frac{A}{D}Mn^{M-1}v_{\text{user}}.$$

Appendix C: The Proof of Theorem 3.3

The probability of all nodes on the i-th level being destroyed is $\prod_{j=1}^{Q_i}(\mathsf{a}_{ij}/\mathsf{d}_{ij}) = (\prod_{j=1}^{Q_i}\mathsf{a}_{ij}) /(\prod_{j=1}^{Q_i}\mathsf{d}_{ij})$. By the inequality of arithmetic and geometric means (AM-GM), to maximize profits for both sides, a_{ij} should be equal to each other and d_{ij} should be all same as well. Then, optimal attack-defense resource allocation strategies for the i-th level are given as follows:

$$\mathsf{a}_{ij}^* = \frac{\mathsf{a}_i}{Q_i}, \quad \mathsf{s}_{\mathsf{a}i}^* = \frac{\mathsf{a}_i}{Q_i}\mathbf{1}_{Q_i}, \quad \mathsf{d}_{ij}^* = \frac{\mathsf{d}_i}{Q_i}, \quad \mathsf{s}_{\mathsf{d}i}^* = \frac{\mathsf{d}_i}{Q_i}\mathbf{1}_{Q_i}.$$

Appendix D: The Proof of Theorem 3.4

By adopting strategies (13), the expectation of the loss function can be expressed as follows

$$\mathbb{E}(L(s_a^*, s_d^*)) = \min_{\mathsf{s}_\mathsf{d}} \max_{\mathsf{s}_\mathsf{a}} \left[1 - \prod_{i=1}^{M}\left(1 - \left(\frac{\mathsf{a}_i}{\mathsf{d}_i}\right)^{Q_i}\right)\right] Q_M v_{\text{user}}. \tag{30}$$

Similar to Remark 3.1, when a level is destroyed, it is not profitable to attack any other level, which means that the attacker should allocate all attack resources to one level. Then, it is reasonable to assume that the attacker takes the following optimal attack strategy

$$\mathsf{s}_\mathsf{a} = \{A\boldsymbol{e}_{iM},\ i = 1, 2, \cdots, M\}. \tag{31}$$

From the defender side, defense resource allocation is first designed to ensure that the loss function keeps invariant under all possible attack strategies. By substituting (31) into (30) and making the loss functions the same, it can be obtained that

$$\left(\frac{A}{\mathsf{d}_1}\right)^{Q_1} Q_M v_{\text{user}} = \left(\frac{A}{\mathsf{d}_2}\right)^{Q_2} Q_M v_{\text{user}} = \cdots = \left(\frac{A}{\mathsf{d}_M}\right)^{Q_M} Q_M v_{\text{user}}. \tag{32}$$

Notice the fact that $\sum_{i=1}^{M}\mathsf{d}_i = D$. The defense resource allocation strategy can be obtained by the following equation

$$\sum_{j=1}^{M}\left(\frac{\mathsf{d}_i}{A}\right)^{\frac{Q_i}{Q_j}} = \frac{D}{A}. \tag{33}$$

If the defender takes a strategy other than (33), there exists such a level whose allocated defense resources are less than those satisfying (33). If all attack resources are allocated to attack this level, the loss function becomes greater. Hence, the robust optimal defense strategy is (33).

If the attacker does not take the strategy defined by (31), it is assumed to divide the attack resources into two parts: αA and $(1-\alpha)A$, $0<\alpha<1$ and these two parts are applied to attack the i-th and j-th levels. Then, the loss function becomes

$$\begin{aligned} &\left[1 - \left(1 - \left(\frac{\alpha A}{\mathsf{d}_i}\right)^{Q_i}\right)\left(1 - \left(\frac{(1-\alpha)A}{\mathsf{d}_j}\right)^{Q_j}\right)\right] Q_M v_{\text{user}} \\ &< \left[\alpha^{Q_i}\left(\frac{A}{\mathsf{d}_i}\right)^{Q_i} + (1-\alpha)^{Q_j}\left(\frac{A}{\mathsf{d}_j}\right)^{Q_j}\right] Q_M v_{\text{user}} \\ &< \left[\alpha\left(\frac{A}{\mathsf{d}_i}\right)^{Q_i} + (1-\alpha)\left(\frac{A}{\mathsf{d}_i}\right)^{Q_i}\right] Q_M v_{\text{user}} = \left(\frac{A}{\mathsf{d}_i}\right)^{Q_i} Q_M v_{\text{user}}. \end{aligned} \tag{34}$$

By continuing this operation, it can be proved that the division of the attack resources leads to a reduction in the loss function. Therefore, under condition (33), the attack resource allocation strategy defined by (31) is optimal.

Appendix E: The Proof of Theorem 5.1

Assume the defender takes the following strategy for all nodes on the j-th ring of the i-th level

$$\mathfrak{d}_{ijk} = \frac{\mathfrak{d}_{ij}}{6}, \quad k = 1, 2, \cdots, 6, \quad \mathfrak{s}_{\mathfrak{d}ij} = \frac{\mathfrak{d}_{ij}}{6}\mathbf{1}_6. \tag{35}$$

Then, the local loss function of that ring can be calculated as

$$\mathbb{E}(\mathfrak{L}_{ij}(\mathfrak{s}_{\mathfrak{a}ij}, \mathfrak{s}_{\mathfrak{d}ij})) = \sum_{k=1}^{6} \mathfrak{p}_{ijk}\mathfrak{v}_i = \frac{6^{M-i+3}v_{\text{user}}}{\mathfrak{d}_{ij}^3}[\mathfrak{a}_{ij6}\mathfrak{a}_{ij1}\mathfrak{a}_{ij2} + \mathfrak{a}_{ij1}\mathfrak{a}_{ij2}\mathfrak{a}_{ij3} + \cdots + \mathfrak{a}_{ij5}\mathfrak{a}_{ij6}\mathfrak{a}_{ij1}]. \tag{36}$$

The attacker would like to maximize local loss function $\mathfrak{L}_{ij}$ of that ring, which leads to the following optimization problem

$$\begin{cases} \displaystyle\max_{\substack{\mathfrak{a}_{ijk} \in \mathbb{R}^+, \\ k=1,2,\cdots,6}} & \mathfrak{a}_{ij6}\mathfrak{a}_{ij1}\mathfrak{a}_{ij2} + \mathfrak{a}_{ij1}\mathfrak{a}_{ij2}\mathfrak{a}_{ij3} + \cdots + \mathfrak{a}_{ij5}\mathfrak{a}_{ij6}\mathfrak{a}_{ij1} \\ \text{s.t.} & \displaystyle\sum_{j=1}^{6} \mathfrak{a}_{ijk} = \mathfrak{a}_{ij}. \end{cases} \tag{37}$$

By the AM-GM inequality, the maximum value of the objective function is $\mathfrak{a}_{ij}^3/6^2$, and the optimal $\mathfrak{a}_{ijk}$ should satisfy that

$$\mathfrak{a}_{ijk} = \frac{\mathfrak{a}_{ij}}{6}, \quad \mathfrak{s}_{\mathfrak{a}ij} = \frac{\mathfrak{a}_{ij}}{6}\mathbf{1}_6. \tag{38}$$

If the defender does not take strategy (35), by the similar analysis in Theorem 3.1, it can be proved that the loss function becomes greater under the optimal attack strategy defined by (38). Therefore, (35) is the optimal defense resource allocation strategy.

To summarize, the optimal attack-defense strategies for the j-th ring on the i-th level are

$$\mathfrak{a}_{ijk}^* = \frac{\mathfrak{a}_{ij}}{6}, \quad \mathfrak{s}_{\mathfrak{a}ij}^* = \frac{\mathfrak{a}_{ij}}{6}\mathbf{1}_6,$$
$$\mathfrak{d}_{ijk}^* = \frac{\mathfrak{d}_{ij}}{6}, \quad \mathfrak{s}_{\mathfrak{d}ij}^* = \frac{\mathfrak{d}_{ij}}{6}\mathbf{1}_6.$$

And the corresponding local loss function of this ring is

$$\mathbb{E}(\mathfrak{L}_{ij}(\mathfrak{s}_{\mathfrak{a}ij}^*, \mathfrak{s}_{\mathfrak{d}ij}^*)) = 6^{M-i+1}\left(\frac{\mathfrak{a}_{ij}}{\mathfrak{d}_{ij}}\right)^3 v_{\text{user}}.$$

Appendix F: The Proof of Theorem 5.2

Assume the defender distributes resources evenly to each ring on the same level. Because there are 6^{i-2} rings on the i-th level ($i = 2, \cdots, M$), the defender's strategy is

$$\mathfrak{d}_{ij} = \frac{\mathfrak{d}_i}{6^{i-2}}, \quad j = 1, 2, \cdots, 6^{i-2}, \quad \mathfrak{s}_{\mathfrak{d}i} = \frac{\mathfrak{d}_i}{6^{i-2}}\mathbf{1}_{6^{i-2}}. \tag{39}$$

By using the same technique as the one in (34), it can be proved that attacking more than one ring decreases the loss function. Therefore, the attacker should choose the following strategy

$$\mathfrak{s}_{\mathfrak{a}ij} = \{\mathfrak{a}_i \boldsymbol{e}_{k6^{i-2}}, k = 1, 2, \cdots, 6^{i-2}\}. \tag{40}$$

If the defender takes the defense strategy other than (39), there exists a ring j such that $\mathfrak{d}_{ij} < \mathfrak{d}_i/6^{i-2}$. Then, if the attacker allocates all the attack resources (allocated to this level) to the j-th ring, the loss function becomes greater. Therefore, the strategy defined by (39) is an optimal choice for the defender under the attack strategy defined by (40).

Therefore, the optimal strategies for both sides at the i-th level are given as follows

$$\begin{aligned}
&\mathfrak{a}^*_{ijk} = \frac{\mathfrak{a}_{ij}}{6}, \quad \mathfrak{s}^*_{\mathfrak{a}i} = \{\mathsf{a}_i \boldsymbol{e}_{l6^{i-2}}, l = 1, 2, \cdots, 6^{i-2}\},\\
&\mathfrak{d}^*_{ijk} = \frac{\mathsf{d}_i}{6^{i-1}}, \quad \mathfrak{s}^*_{\mathfrak{d}i} = \frac{\mathsf{d}_i}{6^{i-2}} \mathbf{1}_6^{i-2}.
\end{aligned}$$

And the local loss function of the i-th $(i > 2)$ level is

$$\mathbb{E}(\mathfrak{L}_i(\mathfrak{s}^*_{\mathfrak{a}i}, \mathfrak{s}^*_{\mathfrak{d}i})) = 6^{M+2i-5} \left(\frac{\mathsf{a}_i}{\mathsf{d}_i}\right)^3 v_{\text{user}}.$$

Appendix G: The Proof of Theorem 5.3

The previous analysis in Section 4 has concluded that the attacker should gather resources together on one level

$$\mathfrak{s}_{\mathfrak{a}} = \{A\boldsymbol{e}_k,\ k = 1, 2, \cdots, M\}.$$

By the similar proof of Theorem 3.4, the defender should balance the defense resources into every level to avoid leaving any weak section (the expected loss function is the same for each level). Therefore, the robust optimal defense resource allocation strategy satisfies the following equations

$$6^{M-1} \frac{A}{\mathsf{d}_1} v_{\text{user}} = 6^{M-1} \left(\frac{A}{\mathsf{d}_2}\right)^3 v_{\text{user}} = \cdots = 6^{M+2i-5} \left(\frac{A}{\mathsf{d}_i}\right)^3 v_{\text{user}} = \cdots = 6^{3M-5} \left(\frac{A}{\mathsf{d}_M}\right)^3 v_{\text{user}},$$

where the first term is the loss function in the case that the root node is attacked.

By using the same technique in (34), it can also be proved that attacking more than one level leads to a loss function reduction. Therefore, (25) is the optimal attack resource allocation strategy.