Research Article

Security Situation Awareness Assessment of Heterogeneous Cyber-Physical Systems in Multiple Load Mode

Xing Yang,1 Ziyi Xie,2 Zhen Qian,2 Xuhong Zhang,3 Dandan Zhao,2 Songyang Wu,4 Hao Peng,2 Dongtao Zhu,1 and Zhenyu Liang1

1State Key Laboratory of Pulsed Power Laser Technology, Advanced Laser Technology Laboratory of Anhui Province, Electronic Countermeasure Institute, National University of Defense Technology, Hefei 230037, China
2Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua 321004, China
3Zhejiang University and Binjiang Institute of Zhejiang University, Hangzhou, Zhejiang, China
4The Third Research Institute of Ministry of Public Security, Shanghai 201204, China

Correspondence should be addressed to Songyang Wu; wusongyang@stars.org.cn

Received 5 September 2022; Revised 27 September 2022; Accepted 28 September 2022; Published 13 October 2022

Copyright © 2022 Xing Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As the Internet of Things technology develops rapidly, cyber-physical systems (CPSs) have provided critical technologies in the industrial field. A smart grid is a typical application of the CPS, which is formed by the coupling of the power network and communication network. In general, the two networks are heterogeneous. Considering the characteristics of the power network, the ordinary percolation network model is not suitable for the network carrying physical flow. Therefore, we propose an interdependent network model with a load. That is, nodes in the physical network have loaded. Then, we research the security of CPS under the multi-load mode. The rule for node failure is different from the percolation model. When a node’s load exceeds its capacity, the node fails. Through the theoretical analysis, we obtained the iterative equation of the percolation threshold and analyzed it through simulation experiments. We adopt both linear and nonlinear capacity models. It is found that appropriately increasing the average degree of ER network can improve its ability to resist attacks. In contrast, the power exponent of the SF network has less influence on the critical value of network percolation. In addition, we found that increasing the capacity parameter in the linear capacity model can improve the robustness of the network, where the variation of the ER-ER network is more evident than that of the SF-SF network. Increasing the capacity parameter in the nonlinear capacity model can significantly increase the network’s ability to resist attacks. However, due to the increase in economical cost, we can improve the network’s reliability by increasing the node capacity while controlling the cost.

1. Introduction

With the rapid development of the Internet and communication technology, the Internet of Things has attracted widespread attention[1–12]. The Industrial Internet of Things is the deep integration of the Internet of Things technology in industrialization and informatization. In the industrial field, through computing, communication, and control, cyber-physical system [13] provides information services for industrial control systems, such as intelligent perception and dynamic control. Today, the modern industrial development is more and more intelligent and informationized, and CPS provides new opportunities in technology and has been widely used in monitoring and control fields [14], intelligent transportation systems [15, 16], and intelligent aerospace [17].

CPS provides data services through computing resource network and physical resource network. Data transmission becomes increasingly coupled with the increasing integration of physical devices and communication networks. We usually model the CPS as two interdependent networks: the physical network and the communication network [18–20]. Due to the interdependence and complexity of the network [21, 22], the failure of a node in one network will not only
affect the network’s connectivity but also affect the nodes interacting with it in another network. The node failure chain reaction occurs between the two networks, resulting in cascading failures [23]. Therefore, it is necessary to study CPS’s safety and robustness.

Chen et al. [24] employed random network and IEEE Standard Bus test case to model CPSs and studied the robustness of cyber-physical power systems under various attack scenarios. They found that considerable clusters, respectively, in physical power grid and communication network are mutually interdependent to survive in cascading failure. Also, targeted attack disintegrates systems into more clusters than random attack, but with less nodes remaining than random attack. Liu et al. [25] studied a converged railway network composed of railways, regional railways, and urban rail transit. They found that with targeted attacks on the highest connected nodes of the coupled network, the robustness decreased as the number of network layers increased. Peng et al. [26] studied the robustness of cyber-physical systems under deliberate attacks, where nodes between networks are connected in a one-to-many ratio. Under the same parameters, they found that the threshold of preferentially attacking SF network is always smaller than that of preferentially attacking ER network, and the security of network is higher. Yang et al. [27] optimized the modelling method of the cyber-physical system, and the connection ratio of nodes between networks was many-to-many. Under the same attack parameters, they found that the threshold of the ER-ER network is larger than that of the SF-SF network, and the power exponent has little effect on the robustness of the network.

We found that the percolation network model [28–30] is unsuitable for physical flow networks. For example, cascading failures arise from the reorganization of flows in electric power grids [31]. Here, the network links have some fixed capacity, and percolation theory provides an abstracted model of vulnerability and cascades in the power grid but neglects the dynamics of flows and the capacities on links. Therefore, this paper proposes an interdependent CPS model with load [32–34]. We assign initial load and capacity to nodes in the physical network and specify load redistribution rule when nodes fail. In this model, the communication and physical networks have different cascading rules. A node in the communication network survives when it belongs to the giant connected component. In the physical network, the survival of a node considers whether the node’s current load exceeds its capacity. When the node’s load does not exceed its capacity, the node survives. Otherwise, the node fails. On the interdependent physical network and communication network, we analyze the cascading failures of CPS, where the physical network has load characteristics and the communication network has percolation characteristics.

2. Proposed Model

In the network, the load-capacity model [21, 22] allocates a certain initial load and capacity to nodes or edges and redistributes load of faulty nodes according to the load redistribution rule. A general load-capacity model consists of three essential elements: initial load, capacity, and load redistribution. A CPS usually consists of a communication network and a coupled physical network. Nodes inside the network are randomly connected, and the two networks have no degree correlation. We optimize the physical network according to the load-capacity model and assign initial load and capacity to nodes. Then, we build an interdependent CPS model with load, as shown in Figure 1.

We set the network $A$ to be a physical network composed of nodes $\{a_1, a_2, \ldots, a_N\}$, and the number of nodes is $N$. Based on the load-capacity model, we assign an initial load and capacity to each node $a_i$ and define the load redistribution rule:

(i) Initial load: we define $L_i(z) = \alpha \cdot z^{-\eta}$ as the initial load of node $a_i$, where $\alpha$ and $\eta$ are constants and $z$ is the degree of node $a_i$.

(ii) Capacity: load-capacity models include linear and nonlinear load-capacity models. The linear capacity of node $a_i$ is defined as $C_i = (1 + \beta \cdot L_i^0)$, where $\beta > 0$ is the capacity parameter and $L_i^0$ is the initial load of node $a_i$. The nonlinear capacity is defined as $C_i = L_i^0 + \beta \cdot (L_i^0)\gamma$, where $\beta > 0$ and $\gamma > 0$ are the capacity parameters.

(iii) Load redistribution rule: after a node is attacked and fails, its own load will be redistributed to other nodes. There are several redistribution rules: load average redistribution rule for the remaining nodes; load average redistribution rule for neighbour nodes; difference load redistribution rule; initial load redistribution rule [35]. In the network, when a node fails, its neighbor nodes are often the most easily affected, so it is reasonable and practical to redistribute the failed node’s load to its neighbor nodes. In a random network, the degree distribution of nodes is relatively uniform, and evenly distributing the load of the failed node to its neighbor is not easy to cause the failure of the neighbor nodes. So in this paper, we adopt the second allocation rule. Assuming that the load carried by the node $a_i$ before the failure is $L_i^0$, it has $m$ neighbor nodes, and then when $a_i$ fails, each neighbor node $a_j$ received additional payload $\Delta L_{ij} = L_i^0/m$. If the node $a_j$ receives an additional load and the load exceeds its capacity, it will cause the node to fail, and the load of the faulty node will be further redistributed to the neighbor nodes.

In the physical network, the node is functional when its load does not exceed capacity. We set the network $B$ to be a communication network composed of nodes $\{b_1, b_2, \ldots, b_M\}$, and the number of nodes is $M$. In the communication network, the node is functional when it belongs to the giant connected component [36, 37]. Assuming that the initial failure occurs on the network $A$, the load of the failed node is transferred to other nodes according to the load redistribution rule. If a node receives additional load beyond its capacity, that node will also fail,
and its load will be further redistributed to other nodes. In the network B, those nodes connected to the failed nodes in the network A will fail due to the loss of dependent edges. After deleting the faulty node, those nodes not part of the giant connected component will also be deleted. Failed nodes of B, in turn, affect nodes in A, causing cascading failures in the interdependent networks A and B. An illustration of fault propagation is shown in Figure 2.

3. Proposed Method

The conditions for node survival are different in the physical and communication networks, so our methods for calculating the proportion of functional nodes in the giant connected components are also different. In the network A, we define several random variables and events. (1) \( Z_i \) is a random variable and represents the number of neighbor nodes of node \( i \). (2) \( X_i \) is a random variable and represents the number of neighbor nodes that make \( i \) fail by transferring its load. (3) \( O \) is an event and indicates that \( i \) fails due to transferring the extra load of neighbor nodes.

Under the condition of \( X = x \), when the load transferred from \( x \) neighbor nodes plus a load of node \( i \) itself exceeds its capacity, the probability of event \( O \) occurring is 1. Otherwise, it is 0, which is

\[
P(O | X = x) = \begin{cases} 
1, & x > (T - 1) \cdot \alpha \cdot z_i^2 / \sum_0 \alpha \cdot z_i^2 \\
0, & \text{otherwise}.
\end{cases}
\] (1)

Further, under the condition of \( Z = z \), we get the probability of event \( O \):

\[
P(O | Z = z) = \sum_{x=0}^z P(O | X = x) \cdot P(X = x | Z = z).
\] (2)

We define \( u \) to represent the probability that node \( i \) cannot reach the functional component through its neighbors. In the network, when we delete \( (1 - \varphi) \) proportion of nodes, there are two cases where the node does not belong to the functional component. (1) The node is deleted, and the probability is \( (1 - \varphi) \). (2) The node is overloaded and fails due to receiving additional loads from neighbor nodes, with the probability of \( \varphi \cdot u^2 \cdot P(O | Z = z) \). We define the event \( E(\varphi) \) as a node that is not the functional node in the network, and its probability is

\[
P(E(\varphi)) = 1 - \varphi + \varphi \cdot u^2 \cdot P(O | Z = z).
\] (4)

After removing the nodes of \( (1 - \varphi) \), the probability that nodes in the remaining network belong to functional nodes is \( \sum_0 P_d(x) \cdot (1 - P(E(\varphi))) \). \( P_d(x) \) is the probability function of the network degree distribution. In the initial network \( A \), the proportion of functional nodes among remaining nodes is

\[
J(\varphi, A) = \frac{\sum_0 P_d(x) \cdot (1 - P(E(\varphi)))}{\varphi} = \frac{\sum_0 P_d(x) \cdot (1 - u^2 \cdot P(O | Z = z))}{\varphi}.
\] (5)

The expression of \( u \) can be obtained by calculation:

\[
u = \sum_{z=0} Q(z) \cdot (1 - \varphi + \varphi \cdot u^2 \cdot P(O | Z = z)),
\] (6)

where \( Q(z) = (z + 1) \cdot P_d(z + 1)/z \), and then we can obtain the functional node ratio \( J(\varphi, A) \) of the nodes in the network \( A \) after the load is propagated.

According to the theoretical process derived by Buldyrev et al. [38], we consider two interdependent networks A and
Cascading failure process reaches a steady state when the network and then the network is the proportion of remaining functional nodes. We define the variables and . Then, the proportion of surviving nodes in the network is obtained:

\[
\begin{align*}
\phi &= x, \\
\phi &= x. 
\end{align*}
\]

Theorem: The theoretical value can be solved in the equation, but the equation is transcendental and cannot be solved exactly.

### 4. Experiments

In this paper, we adopt two capacity models: linear capacity and nonlinear capacity. Two basic network types, ER-ER and SF-SF [39–41], are used to construct the interdependent CPS. Experiments simulate the changes of nodes in the CPS after being attacked. We output the survival of nodes in physical network A and communication network B while maintaining a steady state. In addition, we also analyze the power exponent and average degree of the network, as well as the influence of the capacity parameters and on the network cascading failures. The networks A and B are constructed according to the node ratio of 1:3, the number of nodes , and . Each node in network A depends on three nodes in network B, and each node in network B is uniquely dependent on one node in network A. We set the number of simulations for each experiment as twenty under different parameters.

#### 4.1. Linear Capacity Model

Under the linear capacity model, we study the effect of average degree of ER network, power exponent of SF network, and capacity parameter on the robustness of the interdependent CPS.

First, we use the ER-ER and SF-SF network models to construct an interdependent CPS network with load
characteristics, and set the constant $\alpha = 1.5$, $\eta = 2$, and the capacity parameter $\beta = 2$.

When the average degree of ER network $k = 2, 4, 6, 8$, as the node attack ratio $(1 - p)$ decreases, in the steady state, the change of the giant connected component size $P_G$ of the networks A and B is shown in Figures (a) and (b). We find that when $k = 2$, the network collapses at a meagre attack ratio. With the increase of the average degree $k$, the network’s threshold $p_c$ has been greatly improved. In particular, when $k \geq 4$, the effect of network defence against attacks increases significantly, but as $k$ continues to increase, the change of network robustness becomes insignificant. Comparing Figures 3(a) and (b) at the same value of $k$, we find that the performance of networks A and B is slightly different. When $k = 4, 6, 8$, under different $p$ values, the size of $P_G$ in network B is very close. But in network A, we can clearly see that when $k$ increases, the size of $P_G$ also increases. In network A, when $k$ increases, the number of neighbors of the node also increases, and the failed node distributes less load to each neighbor, so that the neighbor node is not easy to overload and fail.
When the power exponent of SF network $\lambda = 2, 2.6, 2.8, 3$, as the node attack ratio $(1 - p)$ decreases, $P_G$ changes in networks $A$ and $B$ are shown in Figures 3(c) and 3(d). We found that with the increase of $\lambda$, the survival ratio of network nodes increased, but it was not obvious, and $\lambda$ had less impact on the network robustness. Comparing the ER-ER and SF-SF networks, under certain conditions, we found that the percolation threshold of ER network is smaller than that of the SF network, which indicates that the ER-ER network is more resistant to random failures than the SF-SF network.

Next, we further investigate the effect of capacity parameter $\beta$ on the robustness of the network. We set the average degree $k = 6$ and the power exponent $\lambda = 2.6$. We compared the changes in the survival ratio of network nodes under different capacity parameters $\beta$, as shown in Figure 4.
In the ER-ER network, with the increase of $\beta$, the threshold $p_c$ of the network also increases, indicating that increasing the capacity of nodes can improve the ability of the network to resist attacks to a certain extent. However, in the SF-SF network, the increase of $\beta$ does not significantly improve the network robustness, which means that blindly increasing the capacity of network nodes cannot resist attacks well.

Comparing the two network models, we find that when $\beta$ increases to a larger value, the critical value of network percolation will no longer increase. We speculate that there is a threshold for node capacity. When this threshold is exceeded, no matter how much the node's capacity is increased, it cannot effectively affect the robustness of the network.

4.2. Nonlinear Capacity Model. In this section, we study the security of the CPS network constructed based on the nonlinear capacity model through the same simulation experiments. First, we explore the effects of the average degree $k$ of ER network and the power exponent $\lambda$ of the SF network on network percolation. Set the initial load of node as $L_k(x) = \alpha \cdot x^{-\eta}$, where $\alpha = 1.5$, $\eta = 2$. The capacity of the node is $C_i = L_k^\beta \cdot (L_i^\beta)^{\gamma}$, where $\beta = 0.4$, $\gamma = 0.7$.

When the network type is ER-ER, under different average degrees and node attack ratios, the node survival ratios corresponding to the network A and B are shown in Figures 5(a) and 5(b), respectively. The black triangles correspond to the size of the giant connected component $P_G'$ in each case. We find that when $k < 4$, the survival rate of nodes decreases rapidly, and the ability of the network to resist random failures is poor. When $k \geq 4$, the percolation threshold $p_c$ is around 0.8, and the change is not apparent. Therefore, we speculate that appropriately increasing the average degree of ER network can improve the robustness of the network. When $k \geq 4$, continuing to increase the average degree will not have a good effect.

When the network type is SF-SF, under different power exponents and node attack ratios, the node survival ratios corresponding to the network A and B are shown in Figures 5(c) and 5(d), respectively. We found that the influence of the power exponent on network percolation is relatively weak. When $\lambda$ increases from 2 to 3, the threshold changes between 0.8 and 0.9, and the ability of the network to resist attack is relatively poor.

Next, we explore the effect of capacity parameter $\gamma$ on the network percolation. When the network model is ER-ER, we fix other parameters to remain unchanged, where $\alpha = 1.5, \eta = 2, \beta = 0.4$, and $k = 4$. When the capacity parameter $\gamma$ takes different values, the relationship between the node survival ratio $P_G'$ (in the network A and B) and the different nodes’ attack ratio $(1 - p)$ is shown in Figures 6(a) and 6(b).
We found that when $\gamma = 0.3$, the attack ratio that the network can withstand is around 0.2; when $\gamma = 1.5$, the attack ratio that the network can withstand is around 0.6. With the increase of $\gamma$, the percolation threshold $p_c$ increases, and the ability of the network to withstand random attacks is significantly enhanced.

When the network model is SF-SF, set the power exponent $\lambda = 2.6$, and other parameters are the same as above. Under different capacity parameters $\gamma$, the relationship between $P_G$ (in the network A and B) and the different attack ratio $(1 - p)$ is shown in Figures 6(c) and 6(d). We found that when $\gamma = 0.3$, the attack ratio that the network can withstand is around 0.1; when $\gamma = 1.5$, the attack ratio that the network can withstand is around 0.45. The increase of $\gamma$ has a greater impact on network percolation, which can enhance the ability of the network to resist attacks. However, the increase of $\gamma$ means that the node capacity must be increased, and there is a certain pressure on the economic cost. Therefore, appropriately increasing the node capacity can make the network better resist random attacks in the case to control the cost.

Compared with the ER-ER and SF-SF networks, the ER-ER type network can withstand more attacks under the same capacity parameter $\gamma$. This is because of the characteristics of scale-free networks. The degree value of a small number of nodes is substantial. Once these critical nodes fail, the network often faces more significant risks. Further, we focus on the performance of networks A and B under different capacity parameters. Whether in the ER-ER network or SF-SF network, the size of $P_G$ in network A is similar to that in network B under different $p$. We guess that the nature of the nonlinear capacity model makes the failure effect of nodes in network A similar to those in network B.

5. Conclusions

In this paper, we model a cyber-physical system to study network percolation under different conditions. We obtained the iterative equation of the theoretical network threshold through theoretical analysis and conducted simulation experiments.

We propose a new CPS network model: the physical network has a load characteristic in two interdependent networks. Nodes are assigned loads and capacities, and we determine the load redistribution rule. The node failure rule in the physical network differs from the percolation model. When a node’s load exceeds its capacity, it will fail due to overloading. In addition, we also consider linear and nonlinear capacity models, in which the network behaves slightly differently. We found that the average degree of the ER network can affect the critical value of percolation in the network to a certain extent. In contrast, the power exponent of the SF
parameter linear capacity model, we found that increasing the capacity in improving the network’s ability to resist attacks. In the nonlinear capacity model, we found that increasing the capacity parameter $\beta$ can reduce the percolation threshold and improve the robustness of the network. Among them, the change in the ER-ER network is more evident than in the SF-SF network. In the nonlinear capacity model, we found that increasing the capacity parameter $\gamma$ can reduce the percolation threshold and improve the network’s ability to resist attacks.

**Data Availability**

No data were used to support this study.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**Acknowledgments**

This study was partly supported by the National Key Research and Development Program of China under grant no. 2019YFC0118800, the National Natural Science Foundation of China under grant nos. 62072412, 61902359, 61702148, 2019YFC0118800, the National Natural Science Foundation of China under grant no. 61672468, the Opening Project of Shanghai Key Laboratory of Information Network Security, Ministry of Public Security, under grant no. C20607.

**References**


