Research Article
Cascading-Failures Effect on Heterogeneous Internet of Things Systems under Targeted Selective Attack

Xing Yang, 1 Zhen Qian, 2 Xuhong Zhang, 3 Dandan Zhao 4, 2 Hao Peng 4, 2 Dongtao Zhu, 1 and Zhenyu Liang 1

1 State 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
2 Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua 321004, China
3 Zhejiang University and Binjiang Institute of Zhejiang University, Hangzhou, Zhejiang, China

Correspondence should be addressed to Hao Peng; hpeng@zjnu.edu.cn

Received 27 January 2022; Accepted 24 February 2022; Published 21 March 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.

With the rapid development of the Internet of Things (IoT), the physical system and the network space are further deeply integrated, forming a larger-scale IoT heterogeneous fusion system. The attack mode considered in the security mechanism research of traditional large-scale complex systems is relatively simple; only simple attack types such as random attacks on physical systems or network systems are considered. In addition, existing attack modalities such as selectivity, locality, and distribution cannot fully consider the characteristics of security threats in the IoT system. In this paper, for large-scale heterogeneous IoT system scenarios, attackers can attack network systems or physical systems through cyberspace. We conduct situational awareness analysis on important traffic nodes or backbone nodes and study the cascading failures of two interdependent heterogeneous space systems. In view of the existence of such targeted attack threats in large-scale IoT heterogeneous systems, we focus on security assessment and risk prediction issues. First, this paper analyzes and models different IoT heterogeneous systems. Then using the penetration theory, we analyze the cascading failure process step by step and obtain the critical threshold for system collapse failure. Finally, we further verify the correctness of the theoretical values through simulation to effectively analyze and illustrate the reliability of the parameters affecting the system risk. The experimental results show that the large-scale IoT heterogeneous system presents a first-order discontinuous transition value near the critical threshold and the power-law index of the SF network has little effect on the system security.

1. Introduction

Internet of Things (IoT) system is the result of the integration of global Internet systems with advanced computing, analysis, sensing technology, and Internet connection [1–6]. The Internet of Things provides diversified service applications in smart cities, smart grids, and smart transportation [7]. Its development direction is not only to realize the informatization and intelligence of the manufacturing industry like "Industry 4.0" but also to realize the overall digital transformation of various industries [1, 8–11]. The intelligent infrastructure in the Internet of Things provides specific monitoring and control services [12]. It has had an impact on the processing of information, including the design and manufacture of some computer equipment. Internet of Things is not only a technology but also a method of guiding the development of the Internet and 5G in the future. This new way of thinking can give us the opportunity to understand the physical and online world from different angles [13–16]. With the deep integration of digital and traditional infrastructure, the Internet of Things takes cyberphysical systems (CPS) as the critical technology [8]. CPS provides perception, dynamic control, and information services for modern systems through computing, communication, and control [17–19]. It is widely used in smart grid, transportation, medical, and other industries [20, 21]. CPS emphasizes that the physical device cluster in distributed application system is inseparable from communication. The
interaction between the physical world and the digital world is inseparable from the CPS architecture. Internet of Things system composed of CPS architecture usually consists of two interdependent networks, namely, physical resource and computational resource network [19]. IoT system and CPS architecture can connect network devices from different information and communication systems, and their rapid development has also brought a lot of new potential problems [22–25]. Because cyberphysical systems and the Internet of Things are closely related to physical substances, security is very important for them [2]. In reality, networks with similar functions are often coupled together to build an interdependent structure to obtain better robustness and lower risk. For example, power grids in different regions may be coupled together, or similar financial institutions may be related to lower systemic risk. This highly coupled characteristic brings many risks and challenges, such as cascading failure [26–28]. Attackers destroy cyberspace by attacking physical space [29]. The failure of the physical network triggers other nodes’ failure dependent on the information network, which in turn affects the nodes of the physical network [30]. This cascading failure phenomenon will bring great harm to IoT systems [31]. Therefore, analyzing and evaluating the risk and reliability of this system is very necessary. We model this type of system model as an interdependent network composed of two identical networks and study the dynamics and behavior of the system in the process of cascading failure.

The traditional research on network robustness focused on isolated single networks [32, 33], which is not enough to describe the robustness of interdependent networks. Although some studies are aimed at interdependent networks, most of them are simple one-to-one network connections [34–36]. Starting from the one-to-one interdependence model of Buldyrev [37], scholars began to use this percolation theory method to study the cascade scale of IoT systems [38, 39]. Buldyrev pointed out that the double-layer interdependent network is very fragile, and the phase transition process of the largest connected cluster changes from the second-order phase transition of a single network to the first-order discontinuous transition. The one-to-one dependent model is no longer applicable to the ever-changing IoT systems, and scholars have gradually studied the one-to-many model. Huang [30] proposed a one-to-many model in 2015. Nodes in a computing resource network can be connected to nodes in multiple physical resource networks. It is found that if the proportion of faulty nodes exceeds the threshold, the system will crash. This paper only considers the one-to-many situations and does not consider the mixing proportion and more harmful targeted selective attacks. Reference [40] proposed a method to convert targeted attacks into random attacks, but the connection between networks is still a simple one-to-one connection. Peng [41] studied the cascading failure of interdependent networks under a one-to-many model when they were deliberately attacked but did not consider the mixed proportion. To solve the above problems, we model the IoT system as an interdependent network model with mixed node proportion and study the reliability of IoT systems under the targeted selective attack strategy based on node degree.

Our main contributions in this paper are as follows:

(i) Propose a model based on percolation theory to study the propagation of network fault nodes in heterogeneous Internet of Things systems, which is different from the traditional equal proportion model.

(ii) Deduce the critical value that the system can maintain stability after fault propagation, which will help to understand how faults propagate in an interdependent network.

(iii) Use extensive experimental simulation to analyze the survival of functional nodes after fault propagation in heterogeneous Internet of Things systems under different network topologies.

The sections of this paper are organized as follows. The construction of the system model and a transformation method is described in Section 2. For the cascading failure process, we use mathematical methods to analyze each stage in detail in Section 3. The solution of the theoretical value equation is solved in Section 4, and we have carried out a large number of simulation cases to verify the correctness of the theoretical solution and analyze the key factors affecting system reliability. Section 5 is our conclusion and outlook for the future.

2. Our Proposed Method

The system model will be established in this section. We explain the criterion to measure the system’s robustness: the proportion of the most common subgraph in the network. Moreover, we define the parameter formula of deliberate attack, which is transformed into random attack through percolation theory. After transformation, the security of the IoT system under targeted selective attack strategy can be studied in the way of a random attack.

2.1. Model Construction. We develop a new interdependent system model to capture cascading failures. Our framework consists of two networks, and the two networks are represented by $M$ and $N$, respectively. Both types of networks are the most extensive scale-free networks in real life. The degree distribution of scale-free network is $P_{sf}(k) = k^{-\lambda}$. $\lambda$ represents the power-law exponent. From the previous analysis, the connection modes of the two networks in cyberphysical systems include one-to-one, one-to-many, and many-to-many. In practice, many-to-many situations are common. Moreover, the coupling network system composed of various connection ratios also accounts for the vast majority. Therefore, we establish a coupled IoT system composed of two connection ratios. As shown in Figure 1, the two proportions are 2:1 and 1:1, respectively. We assume that the probability of both connection ratios is 0.5. Then, the ratio of network nodes $M$ and $N$ is 3:2.

When we consider real scenarios, such as cyberphysical systems, most of the initial failures are not random. It may be
due to a targeted attack on important hubs (nodes with a high degree). According to the theory of network science, the size of node degree is the key factor in evaluating the importance of a network node. The greater the degree of a node, the more other nodes connected to it. Once this node is destroyed, the nodes connected to it will be affected. Therefore, we choose to carry out targeted attacks according to the node degree.

After the system is deliberately attacked, the attacked node will no longer have a function and fail. We first adopt the targeted selective attack method to attack the node with the largest node degree. When a node in a network is attacked and fails, the corresponding node in another network will lose function due to interdependence. This process is called cascading failure, as shown in Figure 2. Nodes will not fail and maintain its function only if it satisfies the following two requirements:

(i) The node pertains to the functioning giant component
(ii) The node has interdependent edges

Only functional nodes in the network can continue to survive. When there are no functional nodes in the whole network, the network has completely crashed. As shown in Figure 2, node M1 M3 M2 loses its function after being attacked in the initial stage. M2 also fails because it does not belong to the largest connected cluster in Stage 1. N1 N3, which has lost its dependent edge, is no longer functional in Stage 2. N2 does not belong to the largest connected cluster and fails in Stage 3. Node M4 dependents on N2 lose their interdependent edges and fail in Stage 4. In Stage 5, the nodes in the network are no longer invalid and reach stability. This is the whole process of network cascading failure.

2.2. Methods of Converting Targeted Selective Attack. The critical factor in measuring the robustness of the network is the proportion of the most common subgraph in the network [42, 43]. The more significant the proportion of the maximal pass subgraph, the higher the robustness of the network. Newman et al. made outstanding contributions to the method of solving the most general subgraph [44–46]. They use the tool of generating function to solve the network. According to [46, 47], the generation function of network degree distribution is expressed as

$$G_{M0}(x) = \sum_k P_M(k)x^k,$$

(1)

where $P_M(k)$ is the degree distribution function of network $M$. The degree distribution functions of scale-free network and ER random network are $P_{ER}(k) = \langle k \rangle^k e^{-\langle k \rangle}/k!$ and $P_{SF}(k) = k^{-\lambda}$, respectively, where $\langle k \rangle$ is the average degree of ER network and $\lambda$ is the power-law exponent of scale-free network.

Furthermore, the generating function of the underlying branching processes is

$$G_{M1}(x) = \frac{G'_{M0}(x)}{G_{M0}(1)},$$

(2)

According to Sergey’s paper [37], when the network is subjected to random attacks, the proportion of remaining functional nodes in the network can be expressed by

$$g_M(p) = 1 - G_{M0}[1 - p(1 - f_M)],$$

(3)

where $f_M$ satisfies the transcendental equation $f_M = G_{M1}[1 - p(1 - f_M)].$

The principle of cascading failure is the same because the targeted selective and random attack is different only at the first step. Therefore, we can convert targeted selective attacks into random attacks through mathematical derivation. After the transformation, we can analyze the targeted selective attack according to the analysis method of a random attack. In [40], an equation expresses the probability of node failure:

$$Q_a(k_i) = \frac{(k_i + 1)^\alpha}{\sum_{i=0}^N (k_i + 1)^\alpha},$$

(4)

where $Q_a(k_i)$ implies the probability that node $i$ is attacked at the first time. The larger $\alpha$ is, the more vulnerable the node with a high node degree is to attack.

Mapping targeted selective attacks into random attacks can solve the problem of targeted selective attacks. Through mathematical formula analysis and transformation, the newly obtained node survival proportion function is

$$g_M(p) = 1 - \tilde{G}_{M0}[1 - p(1 - f_M)].$$

(5)

And, $f_M = \overline{G}_{M1}[1 - p(1 - f_M)].$

$G_{M0}(x)$ can be solved by the following equations:

$$\begin{align*}
\tilde{G}_{M0}(x) &= G_{M0}\left(1 + \frac{\tilde{P}}{P} (x - 1)\right), \\
G_{M0}(x) &= \frac{1}{P} \sum_k P(k)t^k x^k.
\end{align*}$$

(6)
So far, the transformation of the targeted selective attack has been completed. Next, we will deduce the critical formula of network collapse after cascade failure.

3. Mathematical Analysis of Cascading Failures

This section uses percolation theory and generation function to deduce the cascading failure of interdependent networks after targeted selective attack. We can get the quantity of remaining functional nodes in each step after the network cascade failure through the analysis. Table 1 shows the meaning of some symbols.

3.1. Initial Attack to Network A

3.1.1. Failure in Network M. After deleting the nodes with \( (1 - p) \) ratio in network M, the quantity of remaining nodes is

\[
N'_{M1} = p \cdot N_M = y'_1 \cdot N_M. \tag{7}
\]

Among them, the number of nodes with functions is

\[
N'_{M1} = g_M(y'_1) \cdot N'_{M1} = y'_1 \cdot g_M(y'_1) \cdot N_M \tag{8}
\]

Therefore, the ratio of functional nodes is shown as follows:

\[
y_1 = y'_1 \cdot g_M(y'_1). \tag{9}
\]

3.1.2. Failure in Network N due to M. Due to the interdependence of network N and network M. The node failure in network M will lead to the subsequent failure of corresponding nodes in network N. From the perspective of model construction, the number of nodes with a ratio of 2:1 accounts for 2/3, and the number of nodes with a ratio of 1:1 accounts for 1/3 in network M. Thus, the quantity of nodes with dependencies in network N is

\[
N_{N2}' = \frac{(2/3) \cdot N_M}{2} \cdot (\gamma_1^2 + 2 \cdot \gamma_1 \cdot (1 - \gamma_1)) \cdot \frac{1}{3} \cdot N_M \cdot \gamma_1
\]

\[
= \frac{1}{2} \cdot (3 \cdot \gamma_1 - \gamma_1^2) \cdot N_N, \tag{10}
\]

\[
y_2 = \frac{1}{2} \cdot (3 - \gamma_1) = \frac{1}{2} \cdot y'_1 \cdot g_M(y'_1) \cdot (3 - \gamma_1).
\]

Among them, the number of nodes with functions is

\[
N_{N2}' = g_N(y'_2) \cdot N_{N2}' = y'_2 \cdot g_N(y'_2) \cdot N_N = y_2 \cdot N_N, \tag{11}
\]

\[
y_2 = y'_2 \cdot g_N(y'_2).
\]

3.1.3. Further Fragment of Network M. The initial connection relationship of the network, the number of nodes with a connection ratio of 2:1 and 1:1 in network N is \( \gamma_1^2/2 \) and \( (3 \cdot \gamma_1 - \gamma_1^2)/2 \) can be calculated, respectively. The quantity of nodes with dependencies in network M is

\[
N'_{M3} = \left( \frac{3 - 2 \cdot \gamma_1}{3 - \gamma_1} + \frac{\gamma_1 \cdot 2}{3 - \gamma_1} \right) \cdot N_N \tag{12}
\]

\[
= \frac{2 \cdot y_2}{3 - \gamma_1} \cdot N_M.
\]

Owing to the fact that the nodes eliminated in the first step do not belong to \( N_M, N_{M1} \) and \( N'_{M3} \), the fraction of nodes removed from \( N'_{M1} \) is the same as the fraction of nodes removed from \( N'_{M1} \), so...
\[
N_{M1} - N'_{M1} = \left(1 - \frac{2 \cdot \gamma_2}{(3 - \gamma_1) \cdot \gamma_1}\right) \cdot N_{M1}
\]
(13)

Then the ratio of removed nodes in the original network is
\[
1 - y'_1 + \left(1 - \frac{2 \cdot \gamma_2}{(3 - \gamma_1) \cdot \gamma_1}\right) \cdot y'_1 = 1 - p \cdot g_N(y'_3).
\]
(14)

So,
\[
y'_3 = p \cdot g_N(y'_3).
\]
(15)

The quantity of functional nodes is
\[
N_{M3} = y'_3 \cdot g_M(y'_3) \cdot N_{M} = y_3 \cdot N_{M},
\]
\[
y_3 = y'_3 \cdot g_M(y'_3).
\]
(16)

### 3.1.4. Cascading Failure in Network N Again

In the third step, node failure will further lead to the loss of function of nodes in network N. Similar to the previous calculation, the number of dependent nodes in network N is
\[
N'_{N4} = \left(\frac{2/3 \cdot N_{N4}}{2}\right) \cdot \left(1 - \frac{(3 \cdot y_3 + y'_3)^2}{2}\right) + \frac{1}{3} N_{M} \cdot y_3
\]
\[
= \frac{1}{2} \cdot (3 \cdot y_3 + y'_3) \cdot N_{N}.
\]
(17)

From \(N_{N2}\) to \(N'_{N4}\), we know
\[
N_{N2} - N'_{N4} = \left[1 - \frac{(3 \cdot y_3 + y'_3)^2}{2}\right] \cdot N_{N2}
\]
\[
= \left[1 - \frac{(3 \cdot y_3 + y'_3)^2}{2}\right] \cdot N_{N2}.
\]
(18)

Then, the ratio of removed nodes in the original network is
\[
1 - y'_2 + y'_2 \cdot \left[1 - \frac{(3 \cdot y_3 + y'_3)^2}{2}\right] = 1 - \frac{1}{2} y'_1 \cdot (3 - y_3) \cdot g_M(y'_3)
\]
\[
= \frac{1}{2} \cdot P \cdot (3 - y_3) \cdot g_M(y'_3).
\]
(19)

So,
\[
y'_4 = \frac{1}{2} \cdot P \cdot (3 - y_3) \cdot g_M(y'_3).
\]
(20)

Through the above analysis, we summarize Table 2, which shows the survival ratio of nodes in each stage of network cascade failure. Therefore, the following recursive equation can be derived:
\[
y'_{2i} = \frac{1}{2} \cdot P \cdot (3 - y_{2i-1}) \cdot g_M(y'_{2i-1}),
\]
\[
y'_{2i+1} = P \cdot g_N(y'_3).
\]
(21)

### 3.2. Initial Attack on Network N

#### 3.2.1. Initial Failure in Network N

If network N is attacked for the first time and the attack proportion is \(1 - p\), the number and proportion of remaining nodes in network N are
\[
N'_{N1} = p \cdot N_N
\]
\[
y'_{N1} = y'_{N1} \cdot N_N,
\]
\[
y'_{N1} = y'_{N1} \cdot g_N(y'_1).
\]
(22)

The number and proportion of functional nodes in the remaining nodes are
\[
N_{N1} = g_N(y'_1) \cdot N'_{N1}
\]
\[
= y'_{N1} \cdot g_N(y'_1) \cdot N_M
\]
\[
= y'_{N1} \cdot N_M
\]
\[
y_1 = y'_{N1} \cdot g_N(y'_1).
\]
(23)

#### 3.2.2. Cascading Failures in Network M Caused by N-Node Failures

After node N fails, some nodes in network M fail because they lose their dependent edges. According to the model construction, the node ratio of network M and N is 3:2, so the quantity and proportion of the remaining nodes are
\[
N'_{M2} = y'_{N1} \cdot N_M \cdot \frac{3}{2}
\]
\[
= y'_{N1} \cdot N_M
\]
\[
y'_{M2} = y'_{N1} \cdot N_M
\]
\[
y'_3 = y_1
\]
\[
y'_3 = y_1 \cdot g_N(y'_1).
\]
(24)
Table 2: The stage of network $M$ and network $N$.

<table>
<thead>
<tr>
<th>Stage 1</th>
<th>Network $M$</th>
<th>Network $N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y_1' = e$</td>
<td>$y_1 = y_1' \cdot g_M(y_1')$</td>
<td>$y_2 = 1/2 \cdot y_1' \cdot g_M(y_1') \cdot (3 - y_1)$</td>
</tr>
<tr>
<td>$y_1 = y_1' \cdot g_M(y_1')$</td>
<td></td>
<td>$y_2 = 1/2 \cdot y_1' \cdot g_N(y_1')$</td>
</tr>
</tbody>
</table>

3.2.3. Further Fragment on Network $N$. The definition variable $q_1 = g_M(y_1')$, where $q_1$ represents the proportion of nodes that finally survive in the second stage network $M$. Since a node in network $N$ is connected to one or two nodes in network $M$, the proportion of remaining nodes in network $N$ is

$$\begin{align*}
N_{M2} &= N_{M2}' \cdot g_M(y_2) \\
&= y_2' \cdot g_M(y_2') \cdot N_M \\
&= y_2 \cdot N_M,
\end{align*}$$

(25)

$$\begin{align*}
y_2 &= y_2' \cdot g_M(y_2').
\end{align*}$$

The quantity of the giant component is

$$\begin{align*}
N_{N3} &= \left[1 - (1 - q_1)^2\right] \cdot \frac{2}{(3 + 1/3 \cdot q_1)} \cdot \frac{2}{3} \cdot N_{M2}' \\
&= \frac{1}{3} \cdot y_2' \cdot (5 \cdot q_1 - 2 \cdot q_1^2) \cdot N_N.
\end{align*}$$

(26)

From $|N_1|$ to $|N_3|$, we obtain

$$\begin{align*}
N_{N1} &= N_{N1}' - \frac{1}{3} \cdot y_1' \cdot g_N(y_1') \cdot (5 \cdot q_1 - 2 \cdot q_1^2) \cdot N_N \\
&= N_{N1}' - \frac{1}{3} \cdot g_N(y_1') \cdot (5 \cdot q_1 - 2 \cdot q_1^2) \cdot N_{N1}' \\
&= \left[1 - \frac{1}{3} \cdot (5 \cdot q_1 - 2 \cdot q_1^2)\right] \cdot N_{N1},
\end{align*}$$

(27)

$$\begin{align*}
N_{N1} - N_{N3}' &= \left[1 - \frac{1}{3} \cdot (5 \cdot q_1 - 2 \cdot q_1^2)\right] \cdot N_{N1}'
\end{align*}$$

Therefore, the total number of points removed in network $N$ is the first stage plus the nodes removed in this stage:

$$\begin{align*}
1 - p &+ p \left[1 - \frac{1}{3} \cdot (5 \cdot q_1 - 2 \cdot q_1^2)\right] \\
&= 1 - p \cdot \frac{1}{3} \cdot (5 \cdot q_1 - 2 \cdot q_1^2).
\end{align*}$$

(28)

At this time, the remaining node scores in network $N$ are

$$\begin{align*}
y_3' &= p \cdot \frac{1}{3} \cdot (5 \cdot q_1 - 2 \cdot q_1^2).
\end{align*}$$

(29)

Among the remaining nodes, the number and proportion of nodes belonging to the most Dalian Tong subgroup are

$$\begin{align*}
N_{N3} &= y_3' \cdot g_N(y_3') \cdot N_N \\
&= y_3 \cdot N_N, \\
y_3 &= y_3' \cdot g_N(y_3').
\end{align*}$$

(30)

3.2.4. More Cascading Failures of Network $M$. Since from $N_{M2}$ to $M_{M4}'$, the deleted nodes in the network are equal to $N_{N3}'$ minus $N_{N3}$, we can get

$$\begin{align*}
N_{M2}' - N_{M4}' &= N_{N3}' - N_{N3} \\
&= (1 - g_N(y_3')) \cdot N_{N3} \\
&= (1 - g_N(y_3')) \cdot N_{N3}.
\end{align*}$$

(31)

According to the theory in [37], in the initial attack node, all deleted nodes do not belong to $N_{M3}$, $N_{M4}$, and $N_{N1}$. Therefore, deleting these nodes from $N_{N3}'$ is equivalent to deleting the same proportion of nodes from $N_{M2}'$:

$$\begin{align*}
N_{M2}' - N_{M4}' &= (1 - g_N(y_3')) \cdot N_{M2}' \\
&= (1 - g_N(y_3')) \cdot y_2 \cdot N_M.
\end{align*}$$

(32)

Then, the proportion of total nodes deleted in the third stage network $M$ is equal to $(1 - g_N(y_3')) \cdot y_2' +$ plus the proportion of nodes deleted in the second stage $1 - y_2'$:

$$\begin{align*}
1 - y_2' + (1 - g_N(y_3')) \cdot y_2' \\
&= 1 - y_2' \cdot g_N(y_3') \\
&= 1 - y_2' \cdot g_N(y_3'),
\end{align*}$$

(33)

$$\begin{align*}
y_4' &= y_4' \cdot g_N(y_4'), \\
N_{M4}' &= y_4' \cdot N_M.
\end{align*}$$
The impact of the fourth stage on network A is equivalent to a random attack, in which \( p \) is replaced by \( y_4' \cdot g_M(y_4') \). The number and corresponding proportion of functional nodes in the network are

\[
N_{M4} = y_4' \cdot g_M(y_4') \cdot N_M
\]

\[= y_5' \cdot N_M, \quad (34) \]

\[y_4 = y_4' \cdot g_M(y_4'). \]

Through the above analysis, we can summarize Table 3 and obtain the following recursive equation:

\[
\begin{align*}
\gamma_{2i} &= p \cdot g_N(\gamma_{2i-1}), \\
\gamma_{2i+1} &= p \cdot \frac{1}{3} \cdot (5 - 2 \cdot g_M(y_{2i}')) \cdot g_M(y_{2i}'').
\end{align*} \tag{35}
\]

In the next section, we will use numerical simulation and other methods to find the solution of (21) and (35). Thus, we can get the critical threshold of the coupled network.

4. **Experiments and Analysis**

This section calculates the critical value of network collapse by image fitting. Then, we further prove the correctness of the theoretical value through case studies. Finally, the conditions impacting the robustness of the network are analyzed by changing the relevant parameters.

4.1. **Theoretical Solution.** When the cascading failure of the network stops, the proportion of remaining functional nodes will not change. At this time, the ratio of remaining functional nodes meets the following equations:

\[
\begin{align*}
\gamma_{2i} &= \gamma_{2i-2} = \gamma_{2i+2}, \\
\gamma_{2i+1} &= \gamma_{2i-1} = \gamma_{2i+3}.
\end{align*} \tag{36}
\]

We define new variables \( x \) and \( y \) to meet

\[
\begin{align*}
y &= y_{2i}, \\
&= \gamma_{2i-2}, \\
&= \gamma_{2i+2} \quad (0 \leq y, y \leq 1), \\
x &= y_{2i+1}, \\
&= \gamma_{2i-1}, \\
&= \gamma_{2i+3}.
\end{align*} \tag{37}
\]

So, (21) and (35) will change by

\[
\begin{align*}
y &= \frac{1}{2} \cdot p \cdot (3 - x \cdot g_M(x)) \cdot g_M(x), \\
x &= p \cdot g_N(y),
\end{align*} \quad (38)
\]

\[
\begin{align*}
y &= \frac{1}{3} \cdot p \cdot (5 - 2 \cdot g_M(x)) \cdot g_M(x), \\
x &= p \cdot g_N(y),
\end{align*} \quad (39)
\]

Excluding \( y \), (38) and (39) will become

\[
x = p \cdot g_N\left[\frac{1}{2} \cdot p \cdot (3 - x \cdot g_M(x)) \cdot g_M(x)\right]. \tag{40}
\]

\[
x = p \cdot g_N\left[\frac{1}{3} \cdot p \cdot (5 - 2 \cdot g_M(x)) \cdot g_M(x)\right]. \tag{41}
\]

It is difficult to find an analytical solution to this equation. Therefore, we get the numerical solution by image fitting. The following equations are used to represent (40) and (41):

\[
\begin{align*}
z &= x, \\
z &= \frac{1}{2} \cdot p \cdot (3 - x \cdot g_M(x)) \cdot g_M(x).
\end{align*} \tag{42}
\]

\[
\begin{align*}
z &= x, \\
z &= \frac{1}{3} \cdot p \cdot (5 - 2 \cdot g_M(x)) \cdot g_M(x).
\end{align*} \tag{43}
\]

As shown in Figure 3, we draw two lines of the system of equations. The point where they are tangent is the numerical solution of the equation. Figures 3(a) and 3(b) show the results of the first attack \( M \) and first attack \( N \), respectively. The network types are SF networks with power-law exponent \( \lambda = 2.6 \) and attack parameter \( \alpha = 1 \). When attacking network \( M \), the seepage threshold \( p_c = 0.586 \), and when attacking network \( N \), the seepage threshold \( p_c = 0.576 \). The network types in Figures 3(c) and 3(d) are ER random networks, the average degree \( \langle k \rangle \) is 4, and the attack parameter \( \alpha = 1 \). The percolation threshold \( p_c \) when attacking network \( M \) is 0.615. It is worth noting that the percolation threshold \( p_c \) when attacking network \( N \) is also 0.615. This shows that when the network type is Er-Er, there is little difference in the percolation threshold between attacking \( M \) first and attacking \( N \) first. In order to prove this conclusion again, we continue to attack \( M \) and \( N \) first under the same other conditions and attack parameter \( \alpha = 2 \). The seepage thresholds are shown in Figures 3(e) and 3(f), with values of 0.663 and 0.66, respectively. The two still have little difference. The above conclusion is verified again.

4.2. **Simulation Results.** We verify the results of theoretical derivation by experiments. The percolation process of interdependent networks under deliberate attack will be simulated. We construct two interdependent networks through the network model in model construction, represented as \( M \) and \( N \), respectively, and the network type is ER-ER or SF-SF. Networks \( A \) and \( B \) are connected in a mixed ratio of 2:1 and 1:1 nodes, and the probability of the connection ratio of the two nodes is 0.5. The internal nodes of networks \( A \) and \( B \) are connected according to the connection mode of ER network and SF network. The attack mode is a deliberate attack according to the node degree. In the initial attack, we will attack network \( M \) or \( N \) and save the remaining nodes when the coupled system reaches a stable
Table 3: The stage of network N and network M.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Network N</th>
<th>Network M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 1</td>
<td>$y_1' = p$</td>
<td>$y_2' = y_1' \cdot g_N(y_1')$</td>
</tr>
<tr>
<td></td>
<td>$y_2 = y_1' \cdot g_N(y_1')$</td>
<td>$y_2 = y_1' \cdot g_M(y_1')$</td>
</tr>
<tr>
<td>Stage 2</td>
<td>$y_3' = 1/3 \cdot p \cdot g_M(y_2') \cdot (5 - 2 \cdot g_M(y_2'))$</td>
<td>$y_3' = 1/3 \cdot p \cdot g_M(y_2') \cdot (5 - 2 \cdot g_M(y_2'))$</td>
</tr>
<tr>
<td></td>
<td>$y_4 = y_3' \cdot g_N(y_3')$</td>
<td>$y_4 = y_3' \cdot g_M(y_3')$</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stage 2i</td>
<td>$y_{2i} = y_{2i-1}' \cdot g_N(y_{2i-1})$</td>
<td>$y_{2i} = y_{2i-1}' \cdot g_N(y_{2i-1})$</td>
</tr>
<tr>
<td>Stage 2i+1</td>
<td>$y_{2i+1} = 1/3 \cdot p \cdot g_M(y_{2i}') \cdot (5 - 2 \cdot g_M(y_{2i}'))$</td>
<td>$y_{2i+1} = 1/3 \cdot p \cdot g_M(y_{2i}') \cdot (5 - 2 \cdot g_M(y_{2i}'))$</td>
</tr>
<tr>
<td></td>
<td>$y_{2i+1} = y_{2i+1}' \cdot g_N(y_{2i+1})$</td>
<td>$y_{2i+1} = y_{2i+1}' \cdot g_N(y_{2i+1})$</td>
</tr>
</tbody>
</table>

Figure 3: Continued.
Figure 3: The change of percolation threshold in different parameters. The solutions of equations (42) and (43) are shown. When $p < pc$, there is no intersection between curve and straight line. When $p > pc$, the curve and straight line have two intersections. When $p = pc$, the curve is tangent to the straight line. $pc$ is the network percolation threshold.

Figure 4: Continued.
state or completely crashes. First, we establish two SF networks in the program. Then, the two networks are connected according to the method in the model construction. Finally, we attack the $(1 - p)$ proportion of nodes in network $M$ according to the value of attack parameter $\alpha$. At each stage of network cascading failure, the quantity of remaining functional nodes in each network will be saved. We carried out 50 experiments on each $p$ value and took the average value. This ensures the accuracy of the experiment to a certain extent.

Figures 4(a) and 4(b) correspond to the verification of theoretical results in Figures 3(a) and 3(b). Figures 4(c) and 4(d) correspond to Figures 3(c)–3(f). The black straight line represents the theoretical value, the attack ratio is $(1 - p)$, the abscissa represents $p$, and the ordinate represents the proportion of remaining nodes in each network when the full network node reaches a stable state. It can be seen from the picture that the first-order discontinuous transition of the network is near the critical value, which verifies the correctness of the theoretical value. It can be seen from the picture that when attacking network $A$ first, the proportion of nodes when networks $M$ and $N$ reach the stable state is different, while when attacking network $N$ first, the proportion of nodes when the network reaches the stable state is very close. Moreover, no matter which network is attacked first, the node proportion of network $N$ is always higher than that of network $M$. Through the previous model analysis, the node ratio of networks $M$ and $N$ is $3:2$, and one or two nodes in a network are connected with one node in network $N$. A node in network $N$ will affect one or two nodes in network $M$, which is why the proportion of nodes in network $M$ is less than that of $N$. When attacking a node in network $M$, if it happens to be a node in the ratio of $2:1$, even if one node is lost, another node remains dependent on network $N$, which protects the nodes in network $N$ to a certain extent.

Comparing Figures 4(a) and 4(c) and Figures 4(c) and 4(d), it can be seen that, under the same attack parameters, the percolation threshold of network type ER-ER is greater than SF-SF. The smaller the percolation threshold, the higher the network robustness, and the system can better resist attacks. From the analysis of network type, it can be seen that a small part of nodes in the SF network have the most edges, while the vast majority of nodes have only fewer edges, and the node degree is power-law distributed. The degree distribution of nodes in ER network is the Poisson distribution. The degrees of most nodes are intermediate, and only a few nodes have large or small degrees. This node distribution law indirectly leads to the failure process of SF network nodes once the SF network is attacked. If a minimal number of high degree nodes are attacked, most of the nodes connected to them will fail, which accelerates SF network node failure.

Next, we take points near the theoretical threshold at an interval of 0.005 and calculate the number of remaining functional nodes corresponding to each point. To study the impact of different network sizes, we also selected four groups of network values with different sizes. With the increase of network scale, the image is closer and closer to the critical threshold in Figure 5. So when the number of networks reaches a particular scale, the drawn image will approximate the critical threshold. This further validates our theoretical results.

Finally, we only change the power-law exponent of the SF network under the same other conditions. From Figure 6(a), we find that when $\lambda$ increases, the network percolation threshold decreases accordingly. This indicates that the robustness of the network is increased. At the same time, we also find that the power-law index has little
influence on the robustness of the network. The network percolation threshold increases with $\alpha$. Although the value of $\alpha$ is less than 0, it will still lead to network collapse. This is different from a single network. This is of great significance for us to learn and improve the reliability of the IoT system.

5. Conclusions and Future Work

This paper simulates the network environment of large-scale heterogeneous Internet of Things systems under the targeted selective attack and decomposes and analyzes the cascading-failures effect on the network based on the network percolation theory. Besides, the theoretical solution and simulation solution of the network cascading-failures process are compared and analyzed through digital simulation. The trend, amplitude change, and attack time of network cascading failures under the attack strategy of targeted selective attack can be observed more clearly intuitively. The experimental results prove the effectiveness and correctness of the method proposed in this paper, which can realize the identification and detection of abnormal data in heterogeneous Internet of Things systems under the targeted selective attack strategy.

The research results provide new research ideas for situational awareness and attack characteristics of heterogeneous Internet of Things systems, which can further improve the security of large-scale Internet of Things systems. In future research, we will use the knowledge graph technology to use its sound mesh structure system and match attack types more quickly and accurately to obtain the attack source, attack type, and other data. In addition, we will use the multidimensional correlation knowledge graph

Figure 5: We selected four groups of networks with different sizes to observe the changes of different network sizes near the percolation threshold. (a, b) The case of attacking network $M$ first and network $N$ first, respectively.

Figure 6: Network seepage threshold under different parameters. (a, b) The influence of power-law index $\lambda$ and attack intensity parameters $\alpha$ on network percolation threshold, respectively.
to perform complex combined network attack threat detection. With the support of the multidimensional correlation representation of the spatiotemporal knowledge graph, it can facilitate the collaborative use of knowledge information such as network assets, vulnerabilities, and attack patterns to realize the large-scale information. The real-time detection and analysis of targeted selective attack data in the IoT systems further improve the robustness and stability.

Data Availability

No data were used to support this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work 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, the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security under Grant AGK2018001, and the Key Lab of Information Network Security, Ministry of Public Security, under Grant no. C20607.

References


