Invulnerability Assessment of Cyber-Physics Systems for Blockchain Environment

Hao Peng[1,2], Zhe Kan[1], Dandan Zhao[1(✉)], Zhonglong Zheng[1], and Feilong Lin[1]

[1] College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, Zhejiang, China
ddzhao@zjnu.edu.cn

[2] Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China

Abstract. Due to the decentralized nature and security attributes of blockchain, cyber-physical systems (CPS) emerge more and more interdependent. However, an important challenge of such interdependent CPS is the cascading failures. Thus, how to analyze the invulnerability of interdependent coupled CPS becomes critical and indispensable. In this paper, we have modeled the interdependent CPS in the blockchain environment, and analyzed the cascading failures process based on the network characteristics. Besides, based on simulation experiments, we analyze the main factor affecting the invulnerability of CPS.

Keywords: CPS system · Cascading failures · Invulnerability analysis · Blockchain

1 Introduction

In recent years, the global industrial Internet is in the critical period of undecided pattern [1–3], the window period of large-scale expansion, and the opportunity period to seize the dominant power. CPS (Cyber-Physical Systems) [4, 5] is the core architecture of the Industrial Internet, a multi-dimensional complex system for integrated computing, network and physical environments. It can make the Internet of things system more reliable, efficient and real-time collaborative.

With the widespread popularity and deep development of CPS systems, such as data exchange between isomerism networks will bring new security problems to cyber-physical systems [6–8]. Blockchain technology [9–11] provides a technical basis for building trusted and realizes peer-to-peer data sharing, coordination and communication based on decentralized credit. CPS systems based on blockchain technology [12, 13] are increasingly being applied to industrial Internet applications. Meanwhile, the CPS system based on blockchain technology has certain security attributes and security guarantees [14]. However, the CPS system for the blockchain environment is a decentralized highly distributed heterogeneous coupled system [15]. Each subsystem should work in coordination with each other through wired or wireless communication [16]. According to the computer security theory [17], any heterogeneous system that is

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 450–458, 2019.
https://doi.org/10.1007/978-3-030-21373-2_36

not physically connected to the server is untrustworthy. Heterogeneous coupled CPS systems in a blockchain environment have certain vulnerabilities [18].

From the above, the existing CPS system invulnerability analysis mainly focuses on the invulnerability problem of a single CSP system and lacks the invulnerability analysis of the heterogeneous coupled CPS system oriented to the blockchain environment. In this study, we discuss the cascading failure process by modeling and analyzing the heterogeneous coupled CPS in the existing blockchain environment. And through the simulation and comparison experiments, we analyze the main influencing factors affecting the invulnerability of CPS in Blockchain scenario.

2 Related Models and Concepts

In this section, we model the coupled system by analyzing the relationship between multiple networks that make up the coupled CPS in Blockchain environment.

2.1 System Model

The coupled physical network is a coupled network composed of a communication network and a physical network by analyzing the characteristics of the coupled system and some examples of coupled systems in real life [8, 10, 13], and the number of nodes in the communication network is generally larger than the number of nodes in the physical network. In order to qualitatively study and analyze the coupled network, this paper assumes that the connections between the nodes of the two networks are equal connections. This paper specifies that both networks are Scale-Free networks through analyzing the nature of the interdependent CPS systems. The failure or attack of some networks generally occurs in communication networks, and the failure and attack of the network are generally random.

2.2 Basic Concept

When the communication network is attacked, only nodes that satisfy the following two conditions can maintain the function [18].

- A node in one network is connected to at least a node that maintains functionality in another network.
- The node must belong to the largest connected component.

In order to facilitate theoretical analysis, the communication network is represented by A, and the physical network is represented by B. The number of nodes of the communication network and the physical network is represented by N_A and N_B respectively. When a network in coupled network is attacked, the failure of the nodes in one network affects the function of the nodes in the other network. If none of the two networks fails or the two networks completely collapse, the network reaches steady state. This iterative failure process is called cascading failures. Cascading failures are a common failure process in coupled systems. If cascading failures are not controlled, cascading failures can cause severe damage.

3 Theoretical Analyses

In this section, the mathematical analysis of the cascading failures process is performed by using the generation function and percolation theory in network science [5–7]. The generation functions of network A is

$$G_{A0}(z) = \sum\nolimits_k P_A(k) z^k \tag{1}$$

Where $P_A(k)$ is the degree distribution of network A. According to the above description, network A is a scale-free (SF) network, so the degree distribution of network A is subject to a power law distribution. Its degree distribution is:

$$P_A(k) = c \cdot k^{-\lambda} \tag{2}$$

The generating function of the underlying branching processes is

$$G_{A1}(z) = G'_{A0}(z)/G'_{A0}(1) \tag{3}$$

When some nodes are randomly deleted, the degree distribution of the remaining nodes and the generation function of the degree distribution will change. After randomly deleting a node, the number of remaining nodes is $N'_{A1} = p * N_A$. The fraction of nodes that belong to the giant connected component is

$$g_A(p) = 1 - G_{A0}[1 - p(1 - f_A)] \tag{4}$$

The same conclusion can be drawn in Network B.

3.1 Random Attack in Network A

Next, we analyze the change in the number of nodes in each step of the cascading failures process based on the above theory. We assumed that the fraction $(1 - p)$ of nodes fails due to random attack, so the number of remaining nodes is

$$N'_{A1} = p \cdot N_A = \mu'_1 \cdot N_A \tag{5}$$

Which μ'_1 is the fraction of nodes that remaining $\mu'_1 = p$. Then the fraction of nodes that belong to the giant component of network A is

$$N_{A1} = g_A\left(\mu'_1\right) \cdot N'_{A1} = \mu'_1 \cdot g_A\left(\mu'_1\right) \cdot N_A = \mu_1 \cdot N_A \tag{6}$$

3.2 Cascading Failure of Nodes in Network B

In the previous step, we have obtained the number of nodes that maintain the function after cascading failures. Since one node in network B is randomly connected with three nodes in network A, the number of nodes in network B can be obtained.

$$N_{B2}^{'} = \left[1 - (1 - \mu_1)^3\right] \cdot N_B = \left(\mu_1^3 - 3 \cdot \mu_1^2 + 3 \cdot \mu_1\right) \cdot N_B = \mu_2^{'} \cdot N_B \tag{7}$$

The number of nodes belonging to the giant connected component in $N_{B2}^{'}$ is

$$N_{B2} = g_B\left(\mu_2^{'}\right) \cdot N_{B2}^{'} = \mu_2^{'} \cdot g_B\left(\mu_2^{'}\right) \cdot N_B = \mu_2 \cdot N_B \tag{8}$$

3.3 More Cascading Failures in Network A Due to B-Node Failures

Since there is no relationship between intra-network connections and inter-network connections, the number of nodes in network A can be calculated as:

$$N_{A3}^{'} = \mu_2 \cdot N_B \cdot \begin{matrix}[C_3^1 \cdot \mu_1 \cdot (1 - \mu_1)^2 \cdot 1 + \\ C_3^1 \cdot (1 - \mu_1) \cdot 2 + \mu_1^3 \cdot 3]\end{matrix} / \left[1 - (1 - \mu_1)^3\right] \tag{9}$$

From N_{A1} to $N_{A3}^{'}$ we can get

$$N_{A1} - N_{A3}^{'} = \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot N_{A1} \tag{10}$$

Since the deleted nodes do not belong to N_{B2}, N_{A1} and $N_{A1}^{'}$, the fraction of nodes removed from N_{A1} is equal to the removal of the same fraction of nodes from $N_{A1}^{'}$,

$$N_{A1} - N_{A3}^{'} = \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot N_{A1} = \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot N_{A1}^{'} \tag{11}$$

The fraction of total removed nodes is:

$$1 - \mu_1^{'} + \left(1 - g_B\left(\mu_2^{'}\right)\right) \cdot \mu_1^{'} = 1 - \mu_1^{'} \cdot g_B\left(\mu_2^{'}\right) \tag{12}$$

The number of nodes belonging to the giant connected component is

$$N_{A3} = \mu_3^{'} \cdot g_A\left(\mu_3^{'}\right) \cdot N_A = \mu_3 \cdot N_A \tag{13}$$

3.4 Further Cascading Failures in Network B

In the third step, the failure of the A network will further fail the nodes in the network B. Then the number of nodes with dependencies in the remaining nodes is

$$N'_{B4} = \left[1 - (1 - \mu_3)^3\right] \cdot N_B = \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right) \cdot N_B \tag{14}$$

Thus the total number of failed nodes in Network B is

$$1 - \mu'_2 + \mu'_2 \cdot \left[1 - \left(\mu_3^3 - 3 \cdot \mu_3^2 + 3 \cdot \mu_3\right)/\mu_2\right] = 1 - \mu'_1 \cdot \left(\mu_3^2 - 3 \cdot \mu_3 + 3\right) \cdot g_A\left(\mu'_3\right) \tag{15}$$

So

$$\mu'_4 = \mu'_1 \cdot \left(\mu_3^2 - 3 \cdot \mu_3 + 3\right) \cdot g_A\left(\mu'_3\right) \tag{16}$$

Based on the analysis of the cascading failures process in the previous steps, we can get the iterative relationship of the nodes that are deleted from the network at each stage, expressed by the following equation

$$\begin{cases} \mu'_{2i} = \mu'_1 \cdot \left(\mu_{2i-1}^2 - 3 \cdot \mu_{2i-1} + 3\right) \cdot g_A\left(\mu'_{2i-1}\right) \\ \mu'_{2i+1} = \mu'_1 \cdot g_B\left(\mu'_{2i}\right) \end{cases} \tag{17}$$

Which $\mu'_1 = p$, we will detailed analyze the Eq. (17) in the next section.

4 Experimental Simulations

The main content of this section is to solve the iterative equation obtained in the previous analysis process, and we will verify the theoretical results of the obtained theoretical results to ensure the correctness of the analysis conclusion.

4.1 Solution of Equation

Based on the previous analysis, we obtained the iterative relationship between the two networks in the coupled network during the cascading failures process. The network will not split again when the cascading failure stops, we can obtain

$$\begin{cases} \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2} \\ \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} \end{cases} \tag{18}$$

To facilitate the analysis of iterative formulas for cascading failures, we define new variable $y = \mu'_{2i} = \mu'_{2i-2} = \mu'_{2i+2}$ and $x = \mu'_{2i+1} = \mu'_{2i-1} = \mu'_{2i+3} (0 \le \mathrm{x}, \mathrm{y} \le 1)$. So the Eq. (18) can be presented by the following equation. So

$$\begin{cases} y = p \cdot \left((x \cdot g_A(x))^3 - 3 \cdot x \cdot g_A(x) + 3\right) \cdot g_A(x) \\ x = p \cdot g_B(y) \end{cases} \tag{19}$$

For scale-free networks, this equation is difficult to solve, so we use the way of drawing to find an approximate solution. We define new equations $z = x$ and $z = p \cdot g_B\left[p \cdot \left((x \cdot g_A(x))^3 - 3 \cdot x \cdot g_A(x) + 3\right) \cdot g_A(x)\right]$, then we will draw the two lines in the figure, where the two lines are tangent is the solution of the equation.

In Fig. 1, we use $\lambda_A = \lambda_B = 2.8$, and the value of the minimum degree in the network is 3. As the value of p increases, the two lines will be tangent, and the p-value at the time of tangency is the solution of Eq. (19). By calculating the nearest distance between the two lines, we can more accurately find the value of p when the two lines are tangent.

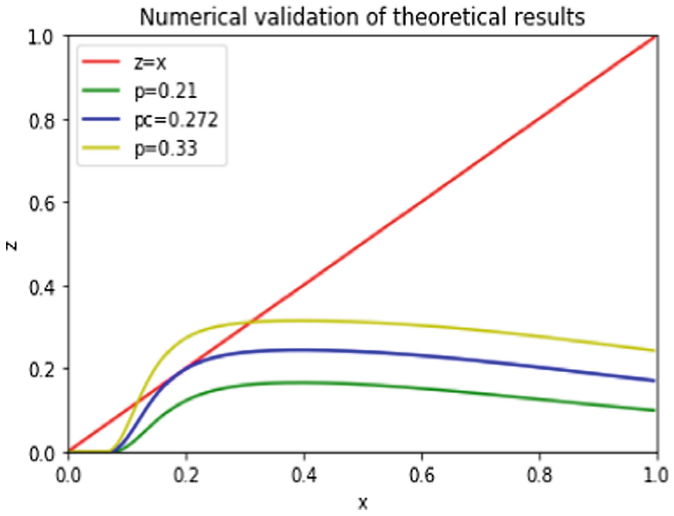

Fig. 1. Solution of equation

4.2 Experimental Verification

In order to verify the correctness of the critical threshold of cascading failures, we use the following simulation settings. Firstly, we construct two scale-free networks based on the specified minimum degree, number of nodes and parameter λ in the simulation experiment. Then, random attacks are represented by randomly deleted nodes. The simulation experiment simulates the process of cascading failure at each step.

In Fig. 2 we compare the variation of the fraction of the remaining nodes in the network when λ takes different values in the end of cascading failures. The black arrow indicates the critical threshold p_c. Meanwhile, the abscissa indicates the proportion of nodes that have not been attacked in the initial stage, and the ordinate indicates the proportion of remaining nodes in the network when the failures stop.

From Fig. 2(a) we see that the network will have the largest connected cluster when the value of p is greater than the critical threshold, which verifies the correctness of our mathematical analysis. In Fig. 2(b), we take $\lambda = 2.4$, and the critical threshold is

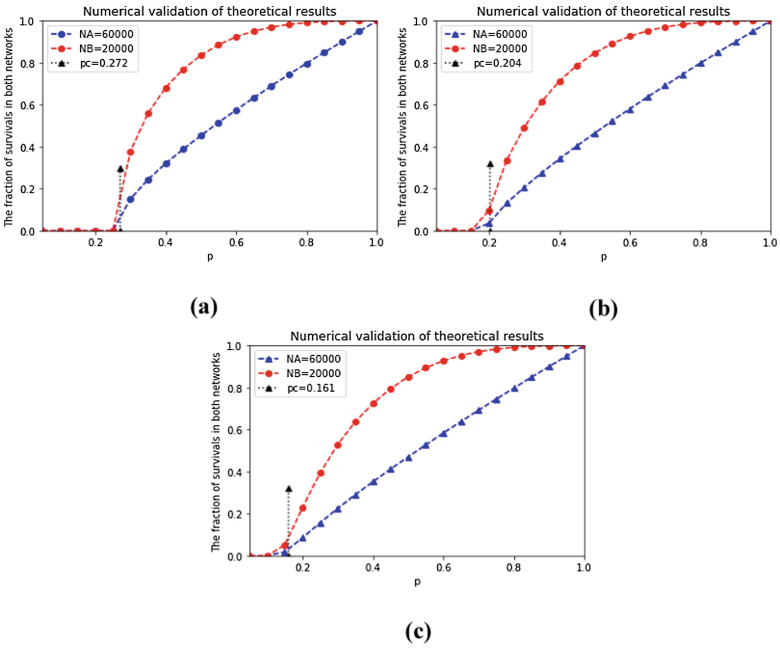

Fig. 2. The fraction of survivals in both networks

$p_c = 0.204$, In Fig. 2(c), we take $\lambda = 2.2$, and the critical threshold is $p_c = 0.161$. The critical threshold p_c decreases as λ decreases.

In order to further verify the correctness of the critical threshold, we take different p values near the critical threshold and calculate the probability of the giant connected component through multiple simulations in Fig. 3. We can see that as the number of

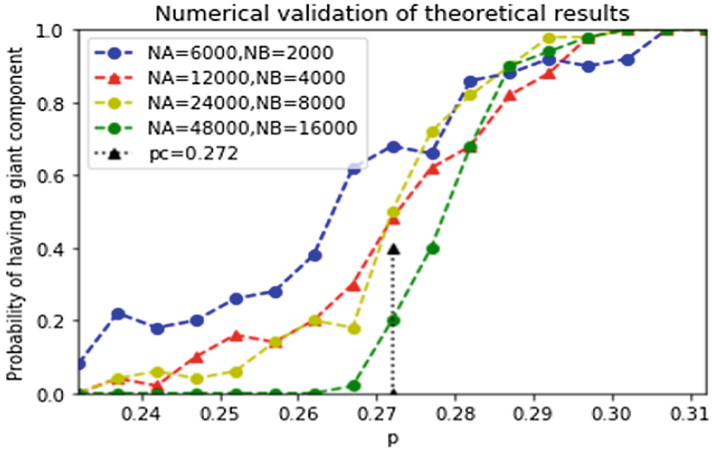

Fig. 3. Probability of having a giant component

nodes increases, the curve becomes steeper near the critical threshold p_c. This phenomenon indicates that the theoretical analysis results are correct. According to the trend of the curve, we can speculate that as the number of nodes increases, the trend of the curve near the critical threshold will become steeper, when the number of nodes is large enough, the network will produce a first-order phase change at the critical threshold. When the values of p and p_c are the same, there may be a maximum connected component or it may not exist. The probability of existence of the giant connected component and the probability of complete collapse are both 0.5.

5 Conclusions

In this paper, we first model the coupled heterogeneous CPS system in a blockchain environment. Then the principle of cascading failure process is analyzed. At the same time, the invulnerability of the system under random attack is compared and analyzed with the simulation process. At last, the analysis of existing research indicates the trend of future research. The invulnerability research of heterogeneous coupled CPS systems in the blockchain environment is still in the initial stage, and there are still many security issues that need further research and discussion.

Acknowledgements. This work was supported by National Natural Science Foundation of China (Grant No. 61602418), Zhejiang Provincial Natural Science Foundation of China (Grant No. LQ16F020002), Social development project of Zhejiang provincial public technology research (Grant No. 2016C33168), MOE (Ministry of Education in China) Project of Humanity and Social Science (Grant No. 15YJCZH125) and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant No. AGK2018001).

References

1. Al-Rubaye, S.: Industrial internet of things driven by SDN platform for smart grid resiliency. IEEE Internet Things J. **6**(1), 267–277 (2017)
2. Li, J.Q.: Industrial internet: a survey on the enabling technologies, applications, and challenges. IEEE Commun. Surv. Tutor. **19**(3), 1504–1526 (2017)
3. Mayer, S.: An open semantic framework for the industrial internet of things. IEEE Intell. Syst. **32**(1), 96–101 (2017)
4. Karnouskos, S.: Stuxnet worm impact on industrial cyber-physical system security. In: Conference on IEEE Industrial Electronics Society, pp. 4490–4494. IEEE (2011)
5. Jia, D.: A survey on platoon-based vehicular cyber-physical systems. IEEE Commun. Surv. Tutor. **18**(1), 263–284 (2017)
6. Colombo, A.W.: Industrial automation based on cyber-physical systems technologies. Comput. Ind. **81**(C), 11–25 (2016)
7. Wei, A.: Adaptive cyber-physical system attack detection and reconstruction with application to power systems. IET Control Theory Appl. **10**(12), 1458–1468 (2016)
8. Pasqualetti, F.: Attack detection and identification in cyber-physical systems – part I: models and fundamental limitations. IEEE Trans. Autom. Control **58**(11), 2715–2729 (2012)

9. Natoli, C.: The balance attack against proof-of-work blockchains: the R3 testbed as an example (2016)
10. Natoli, C.: The balance attack or why forkable blockchains are Ill-Suited for consortium. In: IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 579–590. IEEE (2017)
11. Pass, R., Seeman, L., Shelat, A.: Analysis of the blockchain protocol in asynchronous networks. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 643–673. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_22
12. Dong, Z.: Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. J. Mod. Power Syst. Clean Energy **6**(5), 958–967 (2018)
13. Cebe, M.: Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles (2018)
14. Kosba, A., Miller, A., Shi, E.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: Security & Privacy, pp. 839–858. IEEE (2016)
15. Amin, S.: In quest of benchmarking security risks to cyber-physical systems. IEEE Netw. **27** (1), 19–24 (2013)
16. Shin, D.H.: Cascading effects in interdependent networks. IEEE Netw. **28**(4), 82–87 (2014)
17. Huang, C.: A study on web security incidents in China by analyzing vulnerability disclosure platforms. Comput. Secur. **58**(C), 47–62 (2016)
18. Rungger, M.: A notion of robustness for cyber-physical systems. IEEE Trans. Autom. Control **61**(8), 2108–2123 (2016)