Research on Risk Transmission Process and Immune Strategy of Mine Electric Power Information Network

Caoyuan Ma[1(✉)], Qi Chen[1], Wei Chen[2], Long Yan[1], and Xianqi Huang[1]

[1] China University of Mining and Technology, Beijing, China
{Mcaoyuan,ts18130025a31,ts18130210p31,
ts18060170p3me2}@cumt.edu.cn
[2] Jiangsu Normal University, Xuzhou, China
chenwei@jsnu.edu.cn

Abstract. The power information network is becoming more and more important in the safe and efficient production operation of the mine power system. Meanwhile, the power information network may be subject to security risks, such as malicious virus attacks, which poses challenges to mine safety production. Based on the complex network theory, this paper proposes a complex network model of the power information network. Aiming at the possible attack risk of the power information network, the SIR epidemic model is used to analyze and research on the evolution process of the power information network risk. On this basis, two immunization strategies are proposed to suppress the continuous propagation of power information network security risks. The immunization process of the power information network is simulated to verify the significance of the immunization strategy in the process of power information network security risk transmission.

Keywords: Mine power information network · Complex network · Risk propagation · Infectious disease model · Immune strategy

1 Introduction

As a special information communication network of the power system, the power information network takes responsibility to the power system production and management, as well as plays an important role in the safe and stable operation of the power system [1]. With the development of smart grid, the application of power information network is more and more widely used in mine power production operation. The power information network system for smart mines is a comprehensive information platform, which is proposed to meet the demand of data exchange and informatization. The construction and implementation of the system is able to solve the problem of data sharing and integration between the application systems of the mine power grid and at the same time

Electronic supplementary material The online version of this chapter (https://doi.org/10.1007/978-3-030-63941-9_31) contains supplementary material, which is available to authorized users.

X. Wang et al. (Eds.): 6GN 2020, LNICST 337, pp. 414–423, 2020.
https://doi.org/10.1007/978-3-030-63941-9_31

provide global graphics, global data permissions and data exchange services. Therefore, the information islands problem is solved for many application systems within the mine power grid. Various data resources are able to be interconnected among application systems promoting the informatization of mine power grids.

However, in the process of production operation, the safety margin of the power information network is also continuously reduced, and the power information network has potential hidden dangers. If effective prevention and control strategies are not adopted during the risk contagion, it is easy to cause the local failure at the beginning. Even it develops into an avalanche-like cascading failure, which causes the network to collapse and seriously affects the safe production operation of the power system. This poses a challenge to the construction of a safe and reliable power information network. Therefore, issues of security risks of the power information network should be paid attention to.

From some early analysis of power information network security risk propagation process, the power information network is a typical complex network. The analysis method of complex network added to the analysis process has the better revelation of the overall dynamic propagation behavior process of the information network system. In 1999, Barabási and Albert constructed a complex network model of scale-free networks [2], whose scale-free feature widely existing in various real networks is a typical feature of complex networks. Similarly, the research [3] shows that the power dispatch communication data network is also a scale-free network. Based on the above theory, literature [4] studied the influence of power information network on power system network. As well as the cascading failure propagation process of power information network is analyzed based on the complex network model of scale-free network. The above analysis of the communication of security risks in the information and communication network does not take into account the source and form of the risk nor the propagation law of the risk. Literature [5] did research on the hidden dangers of the power information network originated from malicious attacks, such as hackers, computer viruses, Trojan horses, etc. Therefore, the security protection against these malicious attacks is needed. Literatures [6] studied the spreading of computer viruses in communication networks. Authors found that the spreading of computer viruses and biological viruses are similar, proposed a computer virus SIR infectious disease model. However, the two literatures above analyze the communication network without considering combination of the complex network theory. The topology of the communication network itself is also not taken into account in the process of virus propagation. In addition, the electric power information network has a complex network structure without scale characteristics. The intrusion and spreading of viruses in the network are also random and accidental. These characteristics have an impact on the risk propagation process. However, research of these aspects is not considered in the above literatures. The index of the network reliability, vulnerability and other indicators are the evaluation method of network system security [7]. For the power information network, in order to effectively resist various malicious attacks and ensure the safe and stable operation of the power system, it is necessary to screen out the relatively vulnerable position of the power information network. However, these problems are not quite well presented only depending on the reliability analysis of the network. Therefore, it is necessary to take corresponding measures to conduct vulnerability analysis on the power information network. Literature [8] pointed out that

node importance measurement is of great significance for studying the vulnerability of complex networks. Literature [9] and literature [8] proposed corresponding evaluation methods of node importance of complex networks, which provided new ideas for vulnerability analysis and further immune optimization of complex networks.

This paper analyzes the topology of this particular complex network of power information network. As well as combined with the propagation characteristics of risk, the authors study the SIR model of power information network risk propagation and the optimized immune strategy of power information network. In the end, the simulation is constructed and analyzed.

2 The Foundation of Complex Network Model of Electric Power Information Network

The power information network can be regarded as a complex network which is composed of nodes and lines. A complex network model is established by abstractly simplifying an actual power information network. Therefore, it is easy to analyze the topology structure and risk propagation process of the power information network. At present, complex networks are used to evaluate several basic statistical attributes of their characteristics, including degree, clustering coefficient and shortest path.

(1) The degree of the node. In the network, the degree refers to the number of nodes which are directly connected to the node i. The value of degree is represented by ki. The average degree is the average value of all nodes in the complex network, the value of <k>, shown as,

$$\langle k \rangle = \frac{1}{N} \sum_{i=1}^{N} k_i \tag{1}$$

(2) Degrees distribution. The degree distribution refers to the number of nodes with a degree value of k accounts for the proportion of the total number of nodes in the entire complex network, defined as Pi(k).

(3) The shortest path length. There are usually multiple paths between any two nodes i, j in a complex network. The path with the fewest number of connected edges is defined as the shortest path length, which is denoted by dij. The average value of all the shortest path lengths is the average shortest path length L of this complex network, shown as,

$$L = \frac{1}{N(N-1)} \sum_{ij}^{n} d_{ij} \tag{2}$$

(4) Clustering coefficient C. The clustering coefficient C of complex networks is an important parameter evaluating the aggregation degree of nodes in complex networks. The size of the clustering coefficient indicates the degree of small grouping within the network. The aggregation coefficient of the entire network is:

$$C = \frac{1}{N} \sum_{i=1}^{N} C_i \tag{3}$$

3 Research on the Spatiotemporal Evolution of Security Risks in Electric Power Information

After the nodes of the power information network are randomly invaded by malicious viruses, the risk propagation process of the entire network is usually propagated from a single attacked failure node to its neighbors. Therefore, the neighboring nodes may also have failure. The risk further spreads to its neighboring nodes and gradually spreads to more nodes. If effective preventive measures are not adopted in time, this spreading trend is possible to be very serious. As a result, most nodes have failure due to malicious attacks in the end. Even the entire power information network is systemic collapsed. Since the power network depends on the control of the power information network, there may be a large-scale power outage in the end.

After being maliciously attacked, the nodes of the power information network can return to normal by manually repairing. This scenario is similar to the SIR model in infectious disease theory. Therefore, the SIR model can be used for analogy and fitting when establishing the risk propagation model of the power information network. The SIR model can be used to describe the transmission process, that is, the infected person has immunity after returning to health. Authors study the power information network with a total of N nodes. During the propagation process, N keeps constant. After a node is attacked, it will not be delayed for a long time regardless of a failure or continuing spreading to other nodes, which is similar to the incubation period of infectious diseases. In this case, the nodes of the power information network can be divided into three categories: S-type nodes, I-type nodes and R-type nodes. S-type nodes, which have not been infected, represent susceptible nodes in the power information network. Type I nodes represent nodes that have been infected in the power information network. The risk can continue to spread to other type S nodes from type I nodes. R-type nodes indicate repaired nodes. These nodes have immunity and will not continue to be infected by I-type nodes for a certain period of time. At time t in the propagation process, S(t) is defined as the proportion of S-type nodes to the total number of nodes N. Similarly I(t) and R(t) have the same definition. β represents the probability of infected S-type nodes. γ represents the probability that the type I node returns to normal. The differential equation is:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta S(t)I(t) \\ \frac{dI(t)}{dt} = \beta S(t)I(t) - \gamma R(t) \\ \frac{dR(t)}{dt} = \gamma I(t) \end{cases} \tag{4}$$

The spatio-temporal evolution of risk transmission is analyzed in the complex network of electric power information network by using the SIR infectious disease model. This is certain to obtain the whole process of the network from infection to gradual cure. Figure 1 shows the change process with the time of the proportion of three nodes in the network.

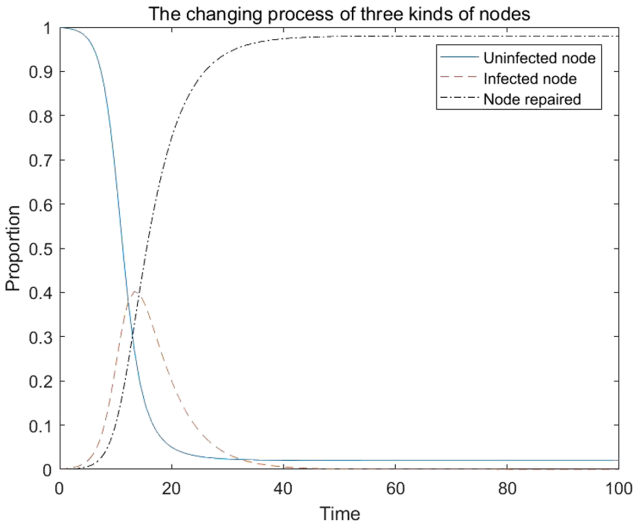

Fig. 1. Three kinds of nodes change curve with time

4 Research on Optimization of Immune Strategy for Power Information Network

For the spread of infectious diseases, the cost-effectiveness of pre-vaccination is much higher than that of post-treatment. There is a similar principle for the risk propagation of the power information network. That is to say, the nodes are selected for pre-immune strengthening, which can greatly reduce the repair cost after the failure of the power information network. Literature [10] mentioned this pre-immunization strategy. If it is an infectious disease of people in the society, the process of vaccination will be affected by the individual's subjective willingness. What should be noticed is that individuals may not be vaccinated in time, even people refuse to vaccinate. So it is not convenient to apply simply the infectious disease immunity model. However, there is no such a complex problem in the power information network. Each node does not have the same subjective willingness as the general population. This ideal objective scenario is convenient for us to apply infectious disease immunity strategies to the power information network.

With the above theoretical conditions, the specific infectious disease immunization strategies are considered. At present, there are three effective immunization strategies: random immunization, acquaintance immunization and targeted immunization.

Random immunization randomly selects some nodes from the network nodes for immunization. There is no additional condition for this kind of immunization. First, acquaintance immunization randomly selects a proportion of nodes from a complex network with a total number of N nodes, and then neighbor nodes are randomly selected from each selecting node to be immunized. Targeted immunization is specific to specific complex network structures. Some nodes play an important role in the transmission process of infectious diseases. If nodes are infected, the intensity of the infectious disease will eventually be stronger. While eventually the spread intensity will be relatively

weaker if they are not infected. This scenario inspires us to identify these important nodes according to the relevant indicators of the nodes. This is the idea of targeted immunity.

Literature [11] pointed out that, in contrast, targeted immunity is a good idea provided that we have mastered the index information of each node of the network. In this paper, the information acquired of the relevant power information network are qualified to use the targeted immune method. Literature [10] presented that these important nodes can be better identified by selecting the node degree as an index. Literature [8] further introduces the topological coincidence degree of neighbor nodes, which are integrated with the node degree to better identify these important nodes.

This paper comprehensively considers the node importance evaluation algorithm in terms of the node degree and the neighboring node's topological coincidence degree. The specific algorithm is as follows:

It is generally acknowledged that the larger the node degree, the more important the node is in the network [12]. However, the importance of a node in a complex network not only depends on the degree of the node, but also depends on the degree of dependence of the neighbor node on the node. What is called neighbor node refers to the low-order neighbor node within two hops. If there is no other connection between the two nodes b and c which are connected to the node a, the information can only be transmitted through the node a. On the condition that the node a fails, the information cannot be transmitted. If there is a common neighbor node d between b and c with the exception of the node a, the central position of the node a weakens, and the robustness of the system increases.

Through the above discussion, the similarity of the node domain can be defined. The higher the similarity of the node domain, the lower the dependence of the entire complex network on the node is. This means that the importance of the node is relatively low. The similarity is defined as sim(b, c). If there is no connection between nodes b and c, it is the equivalent of the result of the first formula. If there is a connection, then it is equal to the second result, which is the value 1. The formula is as follows:

$$sim(b, c) = \begin{cases} \frac{|n(b) \cap n(c)|}{|n(b) \cup n(c)|} \\ 1 \end{cases} \tag{5}$$

A node importance evaluation index LLS(i) based on domain similarity is proposed by combining the degree of the node. The formula is as follows:

$$LLS(i) = \sum\nolimits_{b,c \in n(i)} (1 - sim(b, c)) \tag{6}$$

n(i) represents the neighbor node of the node i. The LLS index comprehensively considers the similarity between the degree of the node and the neighbor node. The larger the LLS value, the more important the node is.

The above are the two power information network immunization strategies. The algorithm flow chart of the two strategies is as follows (Fig. 2):

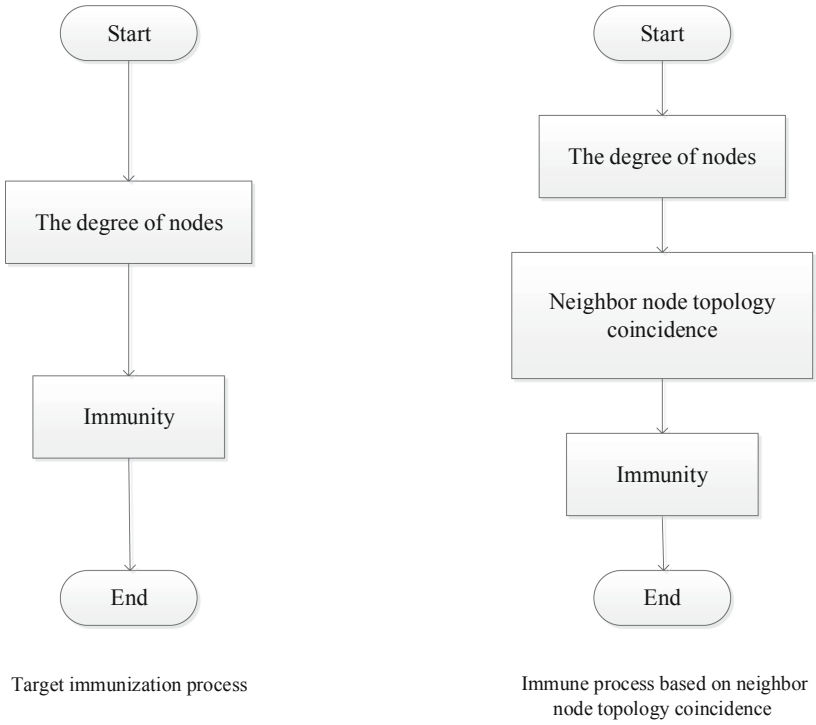

Fig. 2. Comparison of two immunization strategies

5 Analysis of Examples of Electric Power Information Network

Based on the above model and immune strategy, 54-node power information network [13] and 26-node power information network [1] were used for simulation verification separately.

First, the first algorithm of the target immune strategy is applied to the power information network. Degrees are regarded as indicators, the nodes are arranged in order of degree. As well as the degree of each node is obtained. So that the first five nodes from largest to smallest are selected to be immunized (Figs. 3 and 4).

Then the second algorithm is applied to the 54-node power information network. That is to say, the second algorithm is a node importance evaluation algorithm that comprehensively considers the degree of overlap between the node degree and the neighbor node topology. The LLS(i) value of each node is calculated. And the largest five Nodes are to be selected to be immunized.

The non-immunized model and the model after these two immunizations are compared and simulated. The comparison results are shown in the figure (Figs. 5 and 6):

In the figure, the number of initial infected nodes will gradually increase. With optimization of the two immunization strategies, the number of infected nodes is at a lower level and no longer growing. Therefore, the infection process is controlled. The

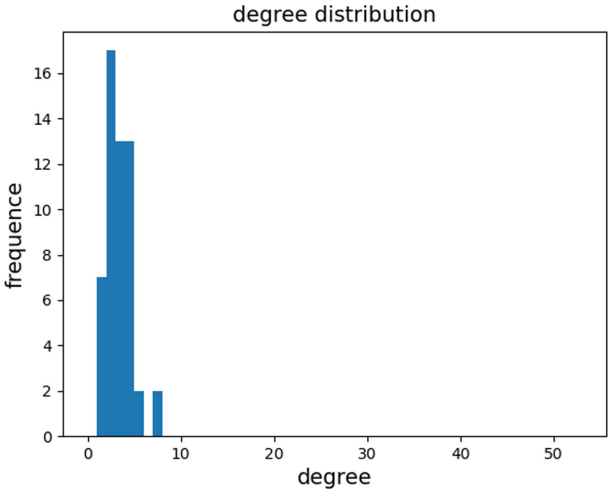

Fig. 3. 54 node degree distribution diagram

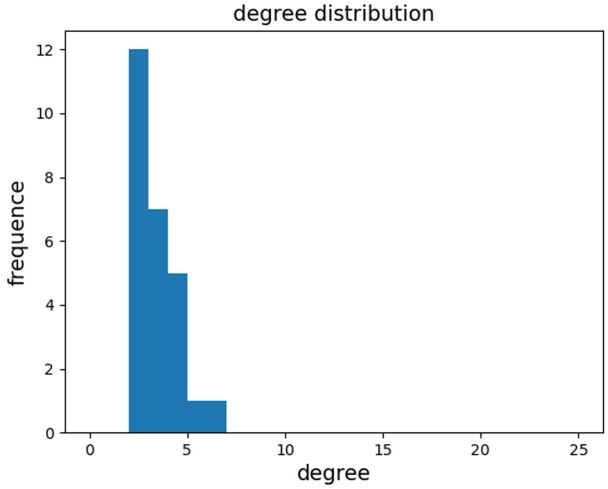

Fig. 4. 26 node degree distribution diagram

total number of infected nodes is effectively reduced by both strategies. An immune strategy that comprehensively considers the degree of node and topological overlapping degree of the neighbor node is better than the target immune strategy, which validates the previous theoretical ideas.

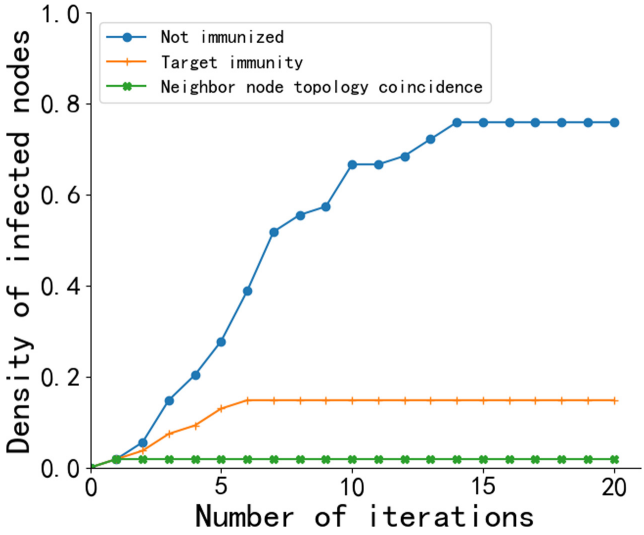

Fig. 5. 54 node network infection node number change diagram

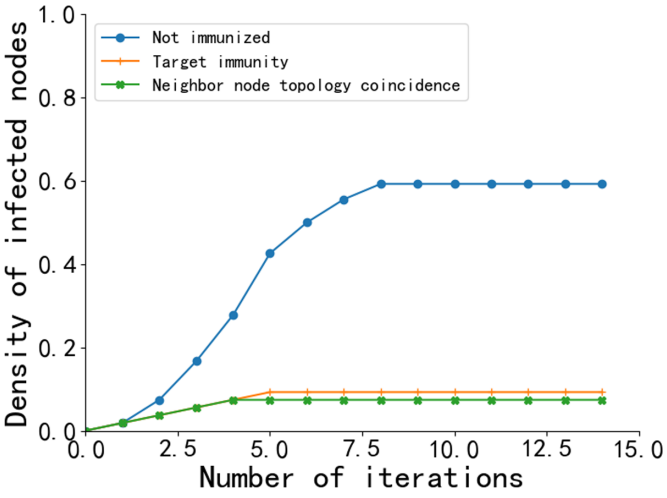

Fig. 6. 26 node network infection node number change diagram

6 Conclusion

Based on the complex network theory, the SIR epidemic model is adopted to analyze and study the evolution process of power information network risk in this paper. The target immune strategy and the immune strategy are used, which comprehensively considers the degree of overlap between the node degree and the neighbor node topology. The power information network immune process is simulated to verify the effectiveness of these two immune strategies in the power information network security risk propagation

process. When the most important nodes are identified more accurately for immune protection, the scale of infection can be further reduced.

References

1. Sun, J., Cui, L.: Business-based vulnerability analysis and evaluation method for power communication network. Power Syst. Prot. Control **45**(24) (2016)
2. Albert, B.: Emergence of scaling in random networks. Science **286**(5439) (1999)
3. Hu, J., Li, Z., Duan, X.: Structural feature analysis of the electric power dispatching data network. Proc. CSEE **29**(4), 53–59 (2009)
4. Cao, Y., Zhang, Y.: Analysis of cascading failures under the influence of power system and communication network interaction. Electr. Power Autom. Equip. **33**(1) (2013)
5. Xie, F.: Design and research of safety protection of electric power monitoring system in new energy power plant. Appl. Energy Technol. **40**(3) (2018)
6. Guo, X.: Spatial propagation mechanism of a kind of SIR computer virus model. J. Anhui Norm. Univ. **40**(3) (2017)
7. Yu, Q.: Research on Risk Spreading Behavior of Complex Networks Based on Risk Spreading Paths and Nodes. Lanzhou University (2017)
8. Ruan, Y.: Evaluation algorithm of node importance of complex network based on domain similarity. Acta Phys. Sin **66**(3) (2017)
9. Xia, L.: Research on Information Propagation Dynamic Modeling and Immune Strategy on Complex Network. Nanjing University of Posts and Telecommunications (2017)
10. Jiang, W.: Overview of precaution and recovery strategies for cascading failures in multilayer networks. Acta Phys. Sin **69**(8) (2020)
11. Liu, X.: Research on Infectious Disease Transmission and Immunization Strategy on Complex Network. Lanzhou University (2015)
12. Liu, W.: Evolution of self-organized critical state of power grid based on weighted network topological entropy. Proc. CSEE **35**(22) (2015)
13. Zhang, K.: Analysis of Influence of Communication Network Based on Dependent Network Theory on Power Network Robustness. Southwest Jiaotong University (2014)