Network Risk Propagation Model Based On Boundary-Center-Point-Search Algorithm

Guo Ping¹,*
¹ Liaoning Jianzhu Vocational College, Liao Yang City, Liao Ning Province, 111000, China
*Corresponding author’s e-mail: guoping3360@126.com

Abstract. Because the power CPS network with community structure has the unique structural characteristics of internal nodes and boundary nodes, the boundary nodes are more likely to cause cascading failures when attacked, which plays an extremely important role in network risk fault propagation. In this paper, the Boundary node is regarded as an important immune object, and these key node targets are quickly identified to take immune measures. A Boundary center-point-search (BCS) algorithm is proposed. According to the disadvantage of the original risk propagation model which ignores the fact that normal nodes can get immunity through artificial means, a risk propagation model is proposed. Compared with other local immune algorithms, the proposed BCS immune algorithm not only can accurately identify the boundary center points between communities, but also has a faster computational speed, which can provide reference for risk propagation control and prevention in large-scale complex networks with incomplete structural information.

1. Introduction
With the rapid development of smart power grid, power System has become the core infrastructure component in today's society. Power System and information System have gradually evolved into the integrated Cyber-physical System (CPS) in a certain connection mode[1]. However, the deep integration between the two also brings some potential problems, which are mainly manifested in that there is no unified modeling method for the huge network formed by the power information physical fusion system[2]; the frequent interaction between information flow and energy flow makes the information system vulnerable to network attacks, and information layer faults may spread in the physical layer, it is easy to cause cascading failure, which eventually leads to power system collapse and blackout[3]. Therefore, it is an urgent problem for power CPS to find effective strategies to suppress network risk propagation[4].

2. Cascading fault mitigation model based on community characteristics
Community structure is the real system or network according to different classification methods, the network nodes are divided into multiple communities, each node belongs to a community to achieve a certain function of the system. The nodes in the community are densely connected, while the nodes outside the community are sparsely connected. Considering the influence of community structure on cascading failure of power information coupling network, the initial load of network node is defined according to the degree of node and neighbor, which can be used to represent the energy flow and information flow of power and information network. The definition of node is shown in formula (1).
\[ L_{ci} = \left( k_{ci} \left( 1 + \sum_{m \in \Gamma_i} (k_{cm} - 1) \right) \right)^\theta \]

\[ L_{pi} = \left( k_{pi} \left( 1 + \sum_{m \in \Gamma_i} (k_{pm} - 1) \right) \right)^\theta \]

(1)

Where, \( K_{ci} \) — Network node degree;
\( \Gamma_i \) — Node maximum neighbor set
\( \theta > 0 \) Is an adjustable initial load distribution parameter

Considering the load redistribution rule of community structure, when the node \( i \) fails, its load \( L_i \) is redistributed to adjacent nodes. If \( j \) is set to a neighbor node \( i \), the load \( j \) allocated is shown in formula (2).

\[ \nabla L_j = L_j \Pi_j = L_j \sum_{m \in \Gamma_j} L_m \]

\[ L_j = \left( k_j \left( 1 + \sum_{m \in \Gamma_j} (k_j - 1) \right) \right)^\theta \]

(2)

\[ L_m = \left( k_m \left( 1 + \sum_{h \in \Gamma_m} (k_h - 1) \right) \right)^\theta \]

Where, \( \Pi_j \) is the load proportion of the original node.

3. Risk propagation model

3.1 A Boundary center-point-search (BCS) algorithm

The basic idea of ACQ acquaintance immunity in local immune algorithm is: select some nodes randomly in the network, and select the neighborhood of these nodes to implement immunity. This method is easy to find nodes with large degree, and is suitable for networks with prominent heterogeneity. Compared with the acquaintance immune method, the BCS local immune method is proposed in order to find these boundary center nodes with high connection edge efficiently.

A Boundary center-point-search (BCS) algorithm is as follows:
1) Select the node \( v_1 \) as the initial point and choose to walk;
2) The node \( v_1 \) choose to get to the node \( v_2 \);
3) Choose to get to the node \( v_3 \), set \( F_2 \) is equal to \( f_{v_1} \cup f_{v_2} \), compare \( f_{v_3} \) with \( F_2 \), all nodes in the set \( f_{v_3} \) are contained in the set \( F_2 \) or have connection edge relationship, and \( v_3 \) is not the final nodes and continue to select other nodes;
4) The node \( v_4 \) can select \( v_5 \) and update \( F_3 \) that it is equal to \( F_2 \cup f_{v_3} \) and compare the relationship network. If all the relationships are contained or connected, node \( v_5 \) is selected to swim;
5) \( F_4 \) includes node \( v_6 \) and \( v_7 \), there is no inclusion or connection relationship with the network \( F_4 \), we will regard \( v_7 \) as the target node and select its neighbor node \( v_8 \) as the boundary center node, and the two will be immune.

3.2 Risk propagation model with local immune mechanism

Based on BCS immune mechanism and SIR (SIR-Avoid-Random) propagation dynamics model, the central node and its neighboring target nodes at the network target boundary are immunized, and then according to SIR model, when the node returns to normal and gets immune with a certain probability, the immune state is obtained. The R node is not at risk of infection, and it will not spread risk to the S-state node. The immune node needs to be removed from the network, and the network is not immune. And adjacency matrix also changed. The SIR-AR model established in this paper is shown in formula (3).
Where, Cell node space $C$: a space with $N$ cells, where cells represent nodes in the system. Cell node finite state set $S$: in SIR-AR model, if a node has normal, infection and immune states, then set $S=\{(0,0),(1,0),(0,1),(1,1)\}$. $(0,0)$ is normal, $(1,0)$ is indicating infection and $(0,1)$ is immune states. The node $i$ is expressed as state $s_i(s_i(t) \in S)$ in time $t$, which $s_i(t)$ contains two sub quantities $s_i(t)\{s_{ix}(t), s_{iy}(t)\}$. The first sub quantity determines whether the node is risk infected, and the second sub quantity determines whether the node is immune. Then, the node $i$ state in time $t$ is shown in formula (4).

$$s_i(t) = \begin{cases} (0,0), & i \in S \\ (1,0), & i \in I \\ (0,1), & i \in R \\ (1,1), & \emptyset \end{cases}$$

First of all, judge whether the node $i$ can be selected with probability $p$, and judge whether it is the node that has been visited, for the node $h_i=1$ is selected, for the node $h_i=0$ is not selected. The rules $h_i$ are shown in formula (5).

$$h_i = \begin{cases} 1, & v_i \not\in V \land p-r > 0 \\ 0, & v_i \in V \lor p-r <= 0 \end{cases}$$

If the node infected by the risk returns to normal at the next moment, it can be immune at the same time. Evolution rules are shown formula (6).

$$s_{ix}(t+1) = \begin{cases} 1, & g_x > 0 \land s_{iy}(t) = 0 \\ 0, & s_{iy}(t) = 1 \end{cases}$$

$$s_{iy}(t+1) = \begin{cases} 1, & g_y > 0 \lor s_{ix}(t) = 1 \\ 0, & g_y \leq 0 \land s_{ix}(t) = 0 \end{cases}$$

Finally, set $S(t), I(t)$ and $R(t)$ at time $t$ are the ratio of the total number of nodes of infection, immunity and normal at the time. Their definitions are shown in equations (7) to (9).

$$I(t) = \frac{1}{N} \sum_{i=1}^{N} s_{ix}(t)$$

$$R(t) = \frac{1}{N} \sum_{i=1}^{N} s_{iy}(t)$$

$$S(t) + I(t) + R(t) = 1$$

4. Calculation examples and analysis

According to SIR-AR model, risk propagation is carried out, and the immune effect of BCS algorithm is compared with AOC and BHD immune algorithm under the same conditions, and the damage degree of BCS algorithm on network connectivity is studied.

4.1 Immune influence of target nodes

Through the cross comparison of the community network formed by the power information network in four coupling modes, the BCS algorithm has a good immune effect, and the difference of the infection range of the immune algorithm is shown in Figure 1.
4

4.2 Analysis of immune efficacy and node vulnerability

By analyzing the data in Figure 1, the average difference between BCS and the other two algorithms under different immune node ratios is obtained. The results are shown in table 1 and table 2.

Table 1. Comparison between acquaintance and BCS immune algorithm

| ACQ-BCS | 0-10% | 10-20% | 20-30% |
|---------|-------|--------|--------|
| CIRL    | 10.65 | 6.65   | 4.72   |
| CADL    | 4.4   | 4.7    | 2.93   |
| CIAL    | 6.1   | 5.9    | 5.9    |
| CAAL    | 7.7   | 7.3    | 5.6    |

Table 2. Comparison between CBF and BCS immune algorithm

| CBF – BCS | 0-10% | 10-20% | 20-30% |
|-----------|-------|--------|--------|
| CIRL      | 8.9   | 7.75   | 4.8    |
| CADL      | 3.1   | 1.83   | 4.79   |
| CIAL      | -0.32 | 4.02   | 3.47   |
| CAAL      | -2.37 | 4.18   | 3      |

It can be seen from tables 1 and 2 that in most cases, the immune performance of BSC algorithm is better than that of ACQ and CBF immune methods.

Node structure vulnerability means that for a given node, the link between some nodes in the network can be disconnected by removing the node and its connecting edge from the network. If there is no connectivity between more nodes after removing a small number of nodes, these nodes are key nodes,
on the contrary, they have strong diffusion or mitigation ability to propagation behavior. The left bar chart shows the vulnerability comparison chart of AOC and BCS immune algorithm nodes, and the right bar chart shows the vulnerability comparison chart of CBF and BCS immune algorithm nodes. It is shown in Figure 2. Compared with the other two immune algorithms, CBS algorithm is easier to make the network collapse.

![Figure 2. Comparison chart of network vulnerability based on immune algorithm](image)

5. Conclusion

In order to prevent the spread of risk failure in the network, a variety of immune algorithms will take the node degree or the shortest path as a reference. However, with the in-depth study of complex networks, it is found that many networks have community structure, in which the boundary point is the bridge connecting the community, which plays a very important role in the communication process. This paper proposes a random walk immune algorithm based on local community structure. BCS algorithm uses neighbor network overlap to distinguish whether the visited node is a boundary node. Based on the heterogeneous distribution characteristics of community network boundary connection, it randomly selects a boundary neighbor of the boundary node, so as to immunize the boundary node and the boundary center node at the same time. And through the actual network, combined with sir-ar propagation model, experiments show that compared with BCS and ACQ immune algorithm, BCS algorithm has better immune effect in community network.

Acknowledgment

This work is supported by Science Research Project of Education Department of Liaoning Province (JYT-L202005).

References

[1] GUO Qinglai, XIN Shujun, SUN Hongbin. et al. Power System Cyber-physical Modelling and Security Assessment: Motivation and Ideas[J]. Proceedings of the CSEE, 2016, 36(6):1481-1489.

[2] Haes, Alhelou, H.; Hamedani-Golshan, M. E.; Njenda, T. C. A survey on power system blackout and cascading events: Research motivations and challenges. Energies, 2019, 12(4), 682.

[3] Chen, B.; Chen, H.; Zhang, Y. Risk Assessment for the Power Grid Dispatching Process Considering the Impact of Cyber Systems. Energies. 2019, 12(6), 1084.
[4] Dai, Q.; Shi, L.; Ni, Y. Risk Assessment for Cyberattack in Active Distribution Systems Considering the Role of Feeder Automation. IEEE Transactions on Power Systems. 2019, 34(4), 3230-3240.