Research on risk prevention and control strategy of power grid CPS system based on intrusion tolerance

Zhanjun Li¹, Bo Hu², Tianqi Lu³, Yuxi Wei⁴, Qingqi Zhao⁵ and Zhiyuan Duan⁶

¹State Grid Liaoning Electric Construction Company, Shenyang, China;
²State Grid Liaoning Electric Power Supply CO., LTD. Shenyang, China;
³State Grid Liaoning Electric Power Company Limited Economic Research Institute, Shenyang, China;
⁴College of information Science and Engineering Northeastern University, Shenyang, China;
⁵State Grid Liaoning Skills Training Center, Shenyang, China
⁶Email: 113439676@qq.com

Abstract. In this paper, an information-physical risk prevention and control framework based on intrusion tolerance technology is proposed, which is a multi-stage in-depth defense system for the risk interaction mechanism and evolution process in the power information-physical fusion system, the aim of this paper is to improve the survivability of the system under attack and minimize the loss caused by the risk through multi-phase defense strategy. At the same time, according to the phase characteristics of risk propagation in CPS, a safe operation state transition model considering intrusion tolerance is established. In order to contain the critical failure events in the risk evolution process of the information-physics fusion system, according to the risk development characteristics of the information-physical system under attack, this paper presents a self-organized critical state identification method, which integrates the characteristics of physical network power flow and information network traffic flow, in order to identify the critical nodes that make CPS system enter the self-organized critical state under network attack. Finally, according to the characteristics of CPS dependent network structure and the self-organized critical characteristics of risk evolution, the protection strategies of strengthening the protection of key nodes, adjusting the coupling state of dependent edges and adding autonomous nodes are formulated, by considering the decision-making model of risk prevention and control strategy in the game of attack and defense, the current defense resources are reasonably allocated.

1. Introduction

The informatization of physical power grids not only improves the level of power automation, improves social production efficiency, and improves user experience, but also brings many hidden dangers to the security of smart grids, especially the cascading failures that alternately propagate between the information network and the physical power grid. Threaten the safe operation of the power system [1-4].

Literature [5] proposed a framework for panoramic security defense of large power grids driven by information with information flow control energy flow as the core, and described in detail the concepts, construction goals, etc., but did not elaborate on the formulation and selection of specific defense strategies. Literature [6] proposed a method of using game method to defend against malicious attacks,
but due to the computational complexity of the algorithm, there is still a certain gap between its practicality. Literature [7] uses countermeasure theory to construct a defense model under the condition that the accident status information of each stage of the grid cascading failure cannot be accurately obtained. Because the information-physical fusion system may lose the monitoring of a certain stage or a certain part of information under a network attack, it has certain reference value for the security defense of CPS. Literature [8] proposed a fraudulent data defense model for power system state estimation based on historical database. From the perspective of state estimation, the countermeasures against false data injection attacks are discussed.

However, the above documents mostly focus solely on the discussion of the defense strategy on the information side or the physical side before the risk occurs. The cross-space risk prevention and control for the actual power grid information-physical system is not completely applicable, because there is no perfect defense system. To withstand the ever-changing cyber attacks, it is urgent to propose a risk prevention and control system that can effectively improve the survivability of the power CPS system under cyber attacks.

2. Analysis of self-organized critical state of power information-physical fusion system

Since the power grid CPS system is an extensive dissipative system, such a system will gradually evolve to a self-organized critical state. Self-organized criticality means that the formation of this state is mainly caused by the interaction between the internal organizations of the system, rather than being controlled or dominated by any external factors [9]. When a self-organizing system is in a critical state, small local changes can be continuously amplified and extended to the entire system. In a critical state, the relationship between the magnitude of the impact of events in the system and its frequency is a power function relationship, which is its most significant feature [10].

The imbalance of the physical network is measured by the power flow entropy. The calculation method of the power flow entropy is as follows:

Define the load rate of the line:

$$O_i = \frac{P_i^{act}}{P_i^{max}}$$  \hspace{1cm} (1)

Among them, $i = 1, 2, \cdots N$.

A set of constant sequence $U = [U_1, U_2, \cdots U_N]$ is given to divide the interval of load rate. Use $N_P^k$ to represent the number of lines in the interval of load rate $O_i \in (U_k, U_{k+1})$, and the proportion of the number of lines on the physical side of the network where the line flow is at $(U_k, U_{k+1})$ is:

$$\tau_k = \frac{N_P^k}{\sum_{k=1}^{N} N_P^k}$$  \hspace{1cm} (2)

Then $\tau_k$ is the probability that the physical side line is in the interval of different load rates. The formula for calculating the power flow entropy of the physical network is as follows:

$$H = \sum_{k=1}^{N-1} \tau_k \ln \tau_k$$  \hspace{1cm} (3)

The imbalance of the information-side network is measured by the entropy of the information service flow, where the service flow is the flow of communication services between the centers of two information nodes.

Define the bandwidth utilization rate of the communication line per unit time as:

$$S_i = \frac{D_i^{act}}{D_i^{max}}$$  \hspace{1cm} (4)

Among them, $i = 1, 2, \cdots N$. 

And a given constant sequence \( V = [V_1, V_2, \ldots, V_n] \) is used to divide the interval of bandwidth utilization. Let \( N_i^c \) represent the number of information lines with bandwidth utilization rate \( \zeta_i \in [V_k, V_{k+1}] \), and the ratio of the number of information line service flows at \( (V_k, V_{k+1}] \) to the number of all information side network lines is:

\[
\chi_k = \frac{N_i^c}{\sum_{i=1}^{n} N_i^c}
\]  

(5)

Then \( \chi_k \) is the probability that the information line is in different bandwidth utilization intervals.

Similarly, the formula for calculating the entropy value of the service flow of the information side network in the above formula is as follows:

\[
H = \sum_{k=1}^{n} \chi_k \cdot \ln \chi_k
\]  

(6)

Drawing lessons from the concept of joint source in information theory, the unbalanced situation of the information side and the physical side is combined to construct a joint source of information-physical system.

The separate probability distributions of information and physical sources are as follows:

\[
\begin{bmatrix}
X \\
P(X)
\end{bmatrix} = \begin{bmatrix}
x_1 & \cdots & x_i & \cdots & x_n \\
P(x_1) & \cdots & P(x_i) & \cdots & P(x_n)
\end{bmatrix}
\]

(7)

\[
\begin{bmatrix}
Y \\
P(Y)
\end{bmatrix} = \begin{bmatrix}
y_1 & \cdots & y_i & \cdots & y_n \\
P(y_1) & \cdots & P(y_i) & \cdots & P(y_n)
\end{bmatrix}
\]

Convert it into a joint source:

\[
\begin{bmatrix}
XY \\
P(XY)
\end{bmatrix} = \begin{bmatrix}
x_i y_1 & \cdots & x_i y_j & \cdots & x_i y_n \\
P(x_i y_1) & \cdots & P(x_i y_j) & \cdots & P(x_i y_n)
\end{bmatrix}
\]  

(8)

Further transformed into the following formula:

\[
\begin{bmatrix}
XY \\
P(X)P(Y)
\end{bmatrix} = \begin{bmatrix}
x_i y_1 & \cdots & x_i y_j & \cdots & x_i y_n \\
P(x_i)P(y_1) & \cdots & P(x_i)P(y_j) & \cdots & P(x_i)P(y_n)
\end{bmatrix}
\]  

(9)

In the above formula, \( X \) refers to the power flow load rate on the physical side, \( P(X) \) is the probability of being in the load interval, that is, \( r_i \); \( Y \) refers to the bandwidth utilization rate of the service flow on the information side, and \( P(Y) \) load rate is the bandwidth utilization rate. The probability is \( \chi_k \).

Finally, the calculation formula of the joint entropy that characterizes the CPS fusion system is as follows:

\[
H_{\text{CPS}} = -\sum_{k=1}^{n} \chi_k \cdot \ln \chi_k \cdot \ln r_i
\]  

(10)

3. Research on prevention and control strategies for improving intrusion tolerance of power information-physical fusion system

3.1. Key node protection strategy

The key node protection strategy is based on the analysis of game theory, through strengthening the security management measures to increase the use of information equipment to reduce the failure probability of information nodes after being attacked. This section proposes a key node protection strategy that considers the structural characteristics of the node and the importance of the node in the self-organized critical state, and can be selected according to the attack strategy of the network attacker.
Comprehensively considering the role of nodes in the critical state of the system, the critical indicators of the current CPS system nodes are as follows:

\[ K_i^p = \omega_1 f_i^s + \omega_2 V_i \]  \hspace{1cm} (11)

Among them, \( \omega_1 \) and \( \omega_2 \) are the vulnerability weight of the node and the critical weight of the node in the self-organized critical state, respectively. The weight can be dynamically assigned according to the network attack mode and strategy.

The calculation formula for the protection ratio of key nodes is as follows:

\[ \kappa = \frac{n_\lambda}{n_{\text{sum}}} \]  \hspace{1cm} (12)

Among them, \( n_\lambda \) is the number of nodes with additional protection measures; \( n_{\text{sum}} \) is the number of nodes in the network.

3.2. Risk prevention and control strategy decision-making model considering offensive and defensive games

The game process between the cyber attacker and the risk defender is as follows:

Based on the state determined by the power grid CPS security state transition model based on the principle of intrusion tolerance, the state set of the system is set to \( S = \{S_1, S_2, \ldots, S_n\} \).

Define the elements of the attacker:

Construct that when the attacker is in the system state \( S_i \), the attacker's strategy set is:

\( G_i = \{g^1_i, g^2_i, \ldots, g^n_i\} \), where \( \phi \in G \) means that the attacker does not initiate an attack.

When the attacker's system state is at \( S_i \), the revenue collection of the attack behavior is:

\( R_i = \{r^1_i, r^2_i, \ldots, r^n_i\} \).

Defining the elements of the defender:

The defense strategy set of the defender when the system state is \( S_i \) is: \( F_i = \{f^1_i, f^2_i, \ldots, f^n_i\} \), where \( \phi \in F \) means that the defender does not adopt any defense strategy.

When the defender's system status is \( S_i \), the defender's revenue collection is \( L_i = \{l^1_i, l^2_i, \ldots, l^n_i\} \).

The above profit of the attacker and the defender is calculated using the load loss of the power information-physical fusion system.

When the system is in state \( S_i \), the profit of the game between the cyber attacker and the power CPS operation defender is as follows:

Attacker's revenue matrix:

\[ R^a = \begin{pmatrix} r_{11}^a & \cdots & r_{1n}^a \\ \vdots & \ddots & \vdots \\ r_{n1}^a & \cdots & r_{nn}^a \end{pmatrix} \]  \hspace{1cm} (13)

The matrix element \( r_{xy}^a \) represents: when the attacker selects strategy \( g_x^a \) and the defender selects strategy \( f_y^D \), the attacker's revenue. \( x \) is the row index, \( y \) is the column index, and \( 0 \leq x, y \leq n \).

Defender's income matrix:

\[ H^d = \begin{pmatrix} l_{11}^D & \cdots & l_{1n}^D \\ \vdots & \ddots & \vdots \\ l_{n1}^D & \cdots & l_{nn}^D \end{pmatrix} \]  \hspace{1cm} (14)

The matrix element \( l_{yx}^D \) represents: the defender selects strategy \( f_x^D \), and the attacker selects strategy \( g_y^D \), the defender's income. \( y \) is the row index, \( x \) is the column index, and \( 0 \leq x, y \leq n \).
Since the game process between the offense and defense is a non-cooperative zero-sum game, therefore:

\[ r_{xy}^A = -l_{yx}^D \]  
\[ R^A = -\left( H^D \right)^T \]  

Then the system is a game state element in the game process between the two parties in the \( S_j \) state:

\[ E_j = \begin{pmatrix} e_{11} & \cdots & e_{ix} \\ \vdots & \ddots & \vdots \\ e_{ni} & \cdots & e_{nx} \end{pmatrix} \]  

Element \( e_{xy} \) in \( E \) is the follow-up benefit of the attacker after the system's operating state changes:

\[ e_{xy} = r_{xy}^A + \sum_{\gamma \in \mathcal{E}_E} P_{\gamma} \left( g_{x}^A, f_{y}^D \right) \cdot E_j \]  

Among them, \( P_{\gamma} \left( g_{x}^A, f_{y}^D \right) \) is the probability that the power information-physical fusion system will transfer from the \( S_i \) state to the \( S_j \) state under the risk caused by the network attack, and \( 0 < P_{\gamma} \left( g_{x}^A, f_{y}^D \right) < 1 \).

Then the attacker's expected revenue from the action strategy is:

\[ E\left( \alpha_i^A, \Omega_j^D \right) = \sum_{\gamma \in \mathcal{G}_E} \sum_{\gamma' \in \mathcal{F}_F} \alpha_i \left( g_{x}^A \right) \cdot \omega_i \left( f_{y}^D \right) \cdot e_{xy} \]  

The strategy that satisfies the following formula can achieve the Nash equilibrium in the current state of the system.

The defense goal of the defender is to maximize its own revenue while minimizing the attacker's revenue, namely:

\[ U^D \left( \alpha_i^A \right) = \min \{ E \left( \alpha_i^A, \Omega_j^D \right) \} \]  
\[ V^D \left( \Omega_j^D \right) = \max \{ U \left( \alpha_i^A \right) \} \]  

The attacker’s goal is to maximize its own revenue while minimizing the defense’s revenue, namely:

\[ U^A \left( \alpha_i^A \right) = \max \{ E \left( \alpha_i^A, \Omega_j^D \right) \} \]  
\[ V^A \left( \Omega_j^D \right) = \min \{ U^A \left( \alpha_i^A \right) \} \]  

The strategy determined by the above formula is the optimal strategy \( \alpha_i^A \) and \( \Omega_j^D \) for both offense and defense.

4. Case analysis
In order to verify that the aforementioned strategy can effectively improve the power CPS system's intrusion tolerance performance under network attacks, this article uses the initial one-to-one coupling method to connect 3 machines and 9-node systems to simulate the implementation of the defense strategy described in this article. After the system is attacked Survivability changes.

First, use the method described in this article to analyze the criticality of the current system nodes and arrange them in descending order. The top 5 critical nodes are shown in Table 1:
Table 1. Part of nodes critical index.

| Sort | Node number | Key indicators |
|------|-------------|----------------|
| 1    | 7           | 2.354          |
| 2    | 5           | 2.147          |
| 3    | 6           | 1.734          |
| 4    | 2           | 1.645          |
| 5    | 9           | 1.639          |

Therefore, the above methods can effectively improve the survivability of the system under network attacks. The following simulation considers the defense resource allocation process of the offensive and defensive game:

The attack scenario is based on the IEEE-57 node system. According to the process described in this article, the game process between the network attacker and the power grid defender is simulated. The system is in an initial normal operating state. The known data of the attacker and the defender are as follows:

See in Table 2, set the attacker's behavior set to \( G_i = \{ \phi, g_i^a \} \), \( g_i^a \) means that the attacker launches a DOS attack; \( \phi \) means that the attacker does not launch an attack. According to the data obtained in the calculation example, the probability set for the attacker to choose the above behavior is: \( \alpha_i^a = \{ \alpha_i(\phi), \alpha_i(g_i^a) \} = \{0.26, 0.74\} \). The revenue collection of the attack is: \( R = \{ 0, r_i^a \} = \{0, 1.17\} \).

Table 2. Attacker’s strategy probability and revenue.

| Attacker strategy                  | Probability of aggressive behavior | The benefits of aggressive behavior |
|-----------------------------------|-----------------------------------|-----------------------------------|
| No attack                         | 0.26                              | 0                                 |
| Launch a DOS attack               | 0.74                              | 1.17                              |

When the defender is in the \( S_i \) state, the set of defense strategies is: \( F_i = \{ \phi, f_i^D, f_2^D, f_3^D \} \), where \( \phi \in F_i \) means that the defender does not adopt any defense strategy; \( f_i^D \) means that the defender implements a redundant configuration of key equipment on the attacked node; \( f_2^D \) means changing the coupling mode of the attacked node The coupling redundancy of the node is set to \( K_{rod} = 0.33 \), and \( f_3^D \) means that the node has an autonomous function.

When the defender is in state \( S_i \), see in Table 3, the probability distribution of the defense strategy adopted by the defender is: \( \Omega_i^D = \{ \alpha_i(\phi), \alpha_i(f_i^D), \alpha_i(f_2^D), \alpha_i(f_3^D) \} = \{0.15, 0.29, 0.45, 0.11\} \) the income set of the defender is \( L_i^D = \{ 0, l_i^D, l_2^D, l_3^D \} = \{0, 1.67, 1.43, 1.15\} \).

Table 3. Defender's strategy probability and revenue.

| Defender strategy                  | Probability of defensive behavior | Defensive behavior gains |
|-----------------------------------|-----------------------------------|-------------------------|
| \( \phi \) No defense             | 0.15                              | 0                       |
| \( f_i^D \) The node implements a redundant configuration of key equipment | 0.29                              | 1.67                     |
| \( f_2^D \) Change node coupling mode | 0.45                              | 1.43                     |
| \( f_3^D \) Node transformation into autonomous node | 0.11                              | 1.15                     |
5. Conclusions
This paper first combines the stage characteristics of risk propagation in the power grid CPS, and develops a safe operating state transfer model considering intrusion tolerance, which lays the foundation for the subsequent allocation of defense resources. Secondly, based on the risk development characteristics of the information-physical fusion system under attack, a comprehensive physical network trend and information network service flow characteristics are proposed. The self-organized critical state identification method is used to identify the key nodes that make the current system enter the self-organized critical state under a certain network attack. Then, according to the characteristics of the dependent network structure of the power grid CPS, a protection strategy was formulated to strengthen the protection of key nodes, adjust the coupling state of interdependent edges, and add autonomous nodes, and determine the current defense by considering the risk prevention and control strategy decision model of the offensive and defensive game. Effective and reasonable allocation of resources. Finally, an example is used to analyze and simulate the allocation of optimal defense strategy.

Acknowledgments
This work is supported by the science and technology project of STATE GRID CORPORATION OF CHINA-Research and Application of Smart Grid Rapid Detection and Response Method under Malignant Data Injection Attack (SGLNJY00GHJS2000044)

References
[1] Guo Qinglai, Xin Shujun, Sun Hongbin, et al 2016 Power system cyber-physical modelling and security assessment:motivation and ideas[J]. Proceedings of the CSEE 36(6) 1481-1489 1761
[2] Wang Yun, Liu Dong, Weng Jiaming, et al 2018 The research of power CPS modeling and simulation verification platform[J]. Proceedings of the CSEE 38(1) 130-136
[3] Liu Wenxia,Gong Qi,Guo Jing,et al 2018 Reliability simulation of ADN cyber-physical system based on hybrid communication network[J]. Proceedings of the CSEE 38(6) 1706-1718
[4] Wang Yufei,Gao Kunlun,Zhao Ting,et al 2016 Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J]. Proceedings of the CSEE 36(6) 1490-1499,1762
[5] Li Baiqing, Liu Daowei, Qin Xiaohui, et al 2016 Information-driven panoramic security defense concept and theoretical framework of large power grids[J]. Proceedings of the Chinese Society of Electrical Engineering 36(21) 5796-5805+6022
[6] Chen Guo, Dong Zhaoyang, Hill D J, et al 2011 Exploring reliable strategies for defending power systems against targeted attacks[J]. IEEE Trans on Power Systems 26(3) 1000-1009
[7] Liu Wenying, Wang Jiaming, Xie Chang, et al 2013 Complex power grid cascading failure defense model based on incomplete information multi-stage countermeasures[J]. Power System Technology 37(4) 1005-1011
[8] Zhu Jie, Zhang Gexiang 2016 Power system state estimation fraud data defense based on historical database[J]. Power System Technology 40(6) 1772-1777
[9] Liu Wenying, Cai Wantong, Zhang Ning, et al 2015 Power grid self-organized critical state evolution based on joint weighted entropy[J]. Proceedings of the Chinese Society of Electrical Engineering 35(6) 1363 -1370
[10] Cao Yijia, Wang Guangzeng, Cao Lihua et al 2011 Self-organized critical state judgment model of complex power grid based on power flow entropy [J]. Automation of Electric Power Systems 35(7) 1-6