Network attack risk assessment of power grid CPS System based on attacker's perspective

Tao Wang¹, Tianmeng Yang¹, Xiao Pan¹, Yuan Meng², Hua Li¹ and Peng Chang²,³

¹ State Grid Liaoning Electric Power Company Limited Economic Research Institute, Shenyang, China;
² College of Information Science and Engineering, Northeastern University, Shenyang, China
³ Email: 1258911858@qq.com

Abstract. Network attack is one of the hidden dangers affecting the safe and stable operation of power systems. In this paper, a potential attack path is established through association algorithm, and the selection probability of the attack path is analyzed comprehensively considering the attacker’s ability, the characteristics of the attack behavior and the characteristics of the target network, and then an improved directed acyclic network attack probability attack graph is established. At the same time, the impact factors of attack action layer and attack target layer are established from the information side and the physical side, and then the incidence of the attack on the whole CPS system is analyzed quantitatively, which improves the comprehensiveness and accuracy of the impact consequence analysis of network attacks. Through the above steps, the potential attack path and the risk value of the system are obtained, and the risk level of the CPS system under the current attack is determined by the fuzzy evaluation method.

1. Introduction
With the construction of power grid automation systems, reliable sensor networks and their deep integration with ubiquitous information networks and energy networks, the traditional power grid is gradually transforming into a power information physical system with wide collaboration and autonomic capacity between information systems and physical systems [1-4]. The development of CPS is bound to be accompanied by the gradual improvement of the dependency degree between interdependent networks, and the faults of unilateral systems may be intercommunicated through the coupling between systems, thus expanding the damage consequences. The fault of one-sided systems may be propagated in the network through mutual coupling between systems, which will enlarge its damage consequence.

At present, in the aspect of risk assessment of power grid CPS, most researches are still remained the risk of fragmented analysis information system and independent physical power grid.

Literature [5] analyzes the security risks in the actual business scenario SCADA system, and believes that it is difficult to guarantee the security of SCADA system in the network environment only by physical isolation, and its remote terminal RTU may be attacked by the Internet, and briefly puts forward measures to improve the system security from the perspective of network security. Literature [6] establishes a mathematical model for firewall and security passwords, the two most
commonly used security protection measures, and evaluates the potential impact of network attack on power system with load loss. However, this paper does not consider the impact of security vulnerability, the internal cause of network risk, on the CPS system risk caused by network attack and the propagation process. Literature [7] carries out quantitative risk assessment on the information security of substation automation system when the communication information system is attacked by malicious attacks. Literature [8] specifically aims risk assessment for information security of power automatic meter reading system. Literature [9] presents a security risk calculation method of intelligent substation system considering the failure effect of application layer equipment application software and power grid management service system software.

Most of the above assessments are only aimed at the risk impact of the physical side under the network attack, and do not comprehensively consider the risk impact of the information side on the cyber-physical fusion system. Therefore, the assessment results are not comprehensive and have certain limitations.

Aiming at these problems above, various types of potential attack path is constructed by association algorithm, and analyzes the selection probability of attack paths based on the characteristics of different attack behaviors. The impact factors of the attack are constructed from the angle of the purpose of the attack, and the risk of the potential attack path of the power grid is obtained. The analysis of the risk level caused by the attack on the power grid CPS system can provide a new perspective for the research on the security analysis and protection methods, and provide accurate basis for the power grid operators to make defensive measures.

2. An improved network attack graph based on the perspective of the attacker

2.1. Improve the basic structure of the network attack graph

The basic structure of the improved network attack graph is shown in Figure 1.

![Network Attack Graph](image)

**Figure 1.** The basic structure of network attack graph.

Firstly, an improved directed acyclic probability attack graph PAG=(N,E,P,C), is established, where N represents the set of nodes in the attack graph. E is the set of directed edges in the attack graph, whose physical significance is the rule used between nodes, namely the causal relationship. P is a probability table attached to each directed edge, and its physical significance is the probability that the attacker chooses this attack path. C is the impact factor of each node in the attack graph, and its physical significance represents the influence of the node on the CPS system after failure.

Model based on graph theory knowledge to the structure design, make the following the attack graph model is set to three layer structures and establish the node set N=A∪I∪UG, from the Angle of attacker, information side and the physical side of relations between weak link.

2.2. Improved network attack graph path creation

The reverse search method can be used to build the attack graph from the attacker's perspective, and the potential attack path can be deduced from the final attack target.
Taking attack target layer node and attack action layer node as an example, the steps to establish the association relationship between nodes are as follows:

1. Obtain the primary and secondary abnormal data indicators and network attack actions in the CPS historical operation database. Mark the primary side abnormal operation indicator as $I_i, I_{i2}, ..., I_{ik}$, mark the second side abnormal operation indicator as $F_j, F_{j2}, ..., F_{jk}$, the network attack action is recorded as $A_1, A_{2}, ..., A_k$, and establish an item collection $I = \{I_1, I_{i2}, ..., I, F_j, F_{j2}, ..., F_jk\}$ and $J = \{F_1, F_{j2}, ..., F_j, A_1, A_{2}, ..., A_k\}$.

2. According to historical operation data abnormal operating indicators listed business set $T = \{t_1, t_{i2}, ..., t_{ik}\}$, each transaction $t_i$ contains an item collection that is a subset of $I$.

3. Scan the abnormal operation indicators of the transaction set $T$, set the support degree according to the specific space and time scene, and iterate mining frequent item set $F$.

4. Association rules are generated from frequent item sets and strong association rules satisfying minimum confidence are found.

### 2.3. Probabilistic prediction model of network attack

1. The difficulty level of utilizing the weak links in CPS system to the attacker

Refer to the establishment of CVSS, the vulnerability rating system of communication network. In view of the weak links in the CPS environment utilizing the difficulty from attacker utilization way $\alpha_{method}$, using complexity $\alpha_{comp}$ and the degree of defense resource allocation of the node $K_i$, these three points to establish a scoring system:

$$E_i = \{1 - (0.05 / K_i)^{\eta} \cdot \alpha_{method} \cdot \alpha_{comp}\}$$  \hspace{1cm} (1)

Among them, $\eta$ is pareto distribution coefficient. The greater the value of $E_i$, the more difficult it is to utilize the weak links of the equipment. The intensity of defense $K_i$, based on the historical attack launched by the attacker, the obtained attack data feedback can be used to determine the defense rating $D_i$ of the current target equipment.

The attacker obtains the general defense level $D_i$, current time scenario $T$ and space scene $S$ of the target network through prior data collection. Consider that there is a certain correlation between the three factors, so the logarithmic synthesis method is used to calculate the defense resource allocation degree of $i$ equipment in the location $S$ within time period $T$ as follows:

$$K_i = \exp(\gamma_1 \ln T_i, + \gamma_2 \ln S_i + \gamma_3 \ln D_i)$$  \hspace{1cm} (2)

2. Failure probability of CPS system equipment after attack

Considering the influence of the repair degree of the weak links of power grid CPS system on the failure probability of the equipment after the attack, if the longer the weak link in the current target CPS system exists, the higher the probability that the link will be found and repaired, the probability of its failure after being attacked will be reduced. Therefore, the average repair degree of weak links in power grid CPS is as follows:

$$R^{\text{av}}_i = \{1 - \exp(t_i / 0.16)^{\beta}\}$$  \hspace{1cm} (3)

Among them, $t_i$ is the existence time of the weak link, $\beta$ is Weibull Distributed parameter. The higher the value of $R^{\text{av}}_i$, the repair degree of the target network is higher, then the probability of its failure after being attacked will be lower.

At the same time, the recovery probability of the infected equipment node can also be expressed in the formula.

3. The penetration degree of current node equipment information to the attacker
For the current attack target area, the number of nodes known by the attacker are sorted according to the accuracy understood by the attacker. Let $O_i$ be the number of the nodes after ordering, and set the number of the node with the most information as 1 and the least as $n' = I_{\text{side}} \cdot N_{\text{sum}}$. Then, quantify the accuracy value $\sigma_i = 1/O_i^{1/\sigma}$ of the attacker's understanding of each information node, the probability of nodes destroyed under the current information accuracy for the attacker is:

$$\tau_i = \frac{\sigma_i}{\sum_{j=1}^{n'} \sigma_j}$$

(4)

Synthesize the difficulty of using the weak link of the above target $E_i$, average repair degree $R_i^{\text{av}}$ and the information factor that the attacker knows about the weak link $\tau_i$. The probability model attached to the $i$-th directed edge is established to indicate that the attacker chooses to attack this path as follows:

$$P_i^{\text{raid}} = \frac{\tau_i}{E_i \cdot R_i^{\text{av}}}$$

(5)

3. Risk analysis of network attack

3.1. Network attack impact factor

(1) Attack action layer impact factor

The variable weight coefficient method is used to characterize the influence of different types of network attacks on the availability, integrity and confidentiality of information, which can provide a basis for subsequent attack behavior discovery and defense strategy formulation. Firstly, the constant weight value $W_i$ of the above three elements is set as 1/3. Secondly, the security indexes of the information equipment are classified and sorted, and then the individual state indexes under the three comprehensive state elements are scored respectively $x_i$. Then get the rating of each comprehensive status index $x_i$, so the variable weight coefficient of the safety index of the information equipment function is as follows:

$$W_i = \frac{W_i}{x_i} \sum_{j=1}^{n} W_j \cdot x_j$$

(6)

Among them, $n$ is the number of single state indexes included in the comprehensive state index; $x_j$ is the score of single status index; $W_j$ is the weight of single status index, in this make it 1/n. In the above formula, $i = \{1,2,3\}$ respectively correspond to the confidentiality, integrity and availability of information equipment functions. The corresponding relationship between the comprehensive state indicators and single state indicators used for information functional impact.

The variable weight coefficient of the three comprehensive indicators is obtained by the above formula, and the functional impact factor of network attack on the $i$-th cyber equipment in the CPS system is obtained by substituting into the following formula:

$$C_i = \ln(\alpha_i e^\alpha + \alpha_i e^\beta + \alpha_i e^\gamma)$$

(7)

(2) Attack target layer impact factor

The impact factor of the attack target layer is to consider the degree of impact on the CPS system after the final removal or failure of the physical side elements when the network attack aimed at destroying the stability of the power grid succeeds.
In this paper, the influence factors of the attack target layer are established by combining the influence factors of structure and function by combining the influence factors of physical side abnormality caused by network attack.

The importance index of electrical topology and the influence index of connectivity rate are established from the perspective of structure.

1) Electrical topology importance factor

Suppose there are \( S \) branches between node \( i \) and node \( j \) on the physical side of the power grid, and the impedance of each branch is \( Z_{1}, Z_{2}, \ldots, Z_{S} \) respectively. According to Kirchhoff's law, \[ U_{i} - U_{j} = IZ_{eq,ij}. \] Then the equivalent impedance \( Z_{eq,ij} \) of the line between node \( i \) and node \( j \) pair is obtained as \[ Z_{eq,ij} = \frac{(U_{i} - U_{j})}{I}. \] For the physical side network with \( M \) nodes and \( N \) branches, the sum of equivalent impedance of all node pairs is defined as the electrical topological quantity of the physical side system \( Z = \sum_{i=1}^{M} \sum_{j=i+1}^{M} Z_{eq,ij}. \)

When a line is mistakenly cut in the network due to network attacks, the electrical topology importance factor of the line in the system is as follows:

\[ C_{T} = \frac{\Delta Z_{k}}{Z} = \frac{\Delta Z_{k}}{\sum_{i=1}^{M} \sum_{j=i+1}^{M} Z_{eq,ij}}. \]

Among them, \( \Delta Z_{k} \) is the circuit equivalent impedance of the branch, the bigger \( C_{T} \) is, the greater the impact of the branch's breaking on the system will be.

2) Connectivity impact factor

It is assumed that before the network attack occurs in the system, the number of branches contained in the largest connected domain in the target network is \( N_{0} \). When a network attack risk event occurs, the number of branches contained in the remaining connected area of the network is \( N_{K} \). The connectivity impact factor of the line is:

\[ C_{G}^{\circ} = \frac{N_{0} - N_{K}}{N_{0}}. \]

The influence factors of voltage and loss of electric quantity are established from the perspective of function.

3) Voltage impact factor

Assume that \( u_{i}^{max} \) and \( u_{i}^{min} \) are the upper and lower voltage lines on the physical side node \( i \) of the system before the network attack occurs. When the network attack risk after the incident, the node voltage quality is affected, cause system node voltage drop in the \( \Delta u_{i} \), the node voltage impact factors is:

\[ C_{v} = \frac{1}{M} \sum_{j=1}^{M} \frac{\Delta u_{i}}{|u_{i}^{max} - u_{i}^{min}|}. \]

3.2. Network attack risk rating

Based on the classical principles of risk assessment, target risk rate=probability of occurrence \( \times \) consequences of the event, and the above analysis results, the risk of CPS system when an attacker chooses to attack a certain path is as follows:

\[ R_{l}^{\text{goal}} = P_{l}^{\text{goal}} \cdot C_{i} \]

\[ R_{l}^{\text{path}} = \prod R_{l}^{i}. \]
\( C_i = \{C'_i, C''_i\} \) is the impact factor of the occurrence of the node event. In the attack graph, the realization of the attack target is the result of the joint action of multi-step node attacks, so the risk that an attacker chooses an attack path is \( R_{\text{path}} \).

Firstly, the total number of the current network attack risk levels is determined as 5 levels, and the fuzzy comprehensive evaluation method is used to classify the risk levels caused by the current network attack. The alternative set in fuzzy space is divided into 5 levels: \( V = \{v_1, v_2, v_3, v_4, v_5\} = \{\text{very low, low, medium, high, very high}\} \).

The isosceles triangle membership function is used to construct the membership function used for operation state grading.

The risk impact index evaluation matrix \( R_i \) and its weight matrix \( \{\mu_1, \mu_2, \mu_3, \mu_4, \mu_5\} \) of the current attack target layer of the network constitute the comprehensive fuzzy subset \( B_i \) of the system risk under the current attack, and its calculation formula is as follows:

\[
B_i = A \circ R_i = (b_{i1}, b_{i2}, b_{i3}, b_{i4}, b_{i5})
\]

\( \circ \) is the adopted fuzzy operator, and \( M (+, \circ) \) model is used.

Finally, the comprehensive fuzzy subset \( \bar{B}_i = (\bar{b}_{i1}, \bar{b}_{i2}, \bar{b}_{i3}, \bar{b}_{i4}, \bar{b}_{i5}) \) of the system under the current attack is obtained, and the maximum membership degree method is used to describe the risk level of the system under the current attack.

4. The example analysis

The information physical interaction node is located in IEEE-57 system, with the upper layer docking to IEEE-57 system information side \( C_{14} \) and the lower layer docking to physical side bus 8, and the mobile attack and defense platform simulating a network attack launched by a network attacker.

The impact factors of the attack in the attack action layer can be obtained, as shown in Table 1:

| Attack type name | Fuzzing attack | DOS attack | Control permission access attacks |
|------------------|----------------|------------|----------------------------------|
| Attack action layer impact factor | \( C'_i = 1.331 \) | \( C'_i = 1.2503 \) | \( \mu_i = 1.4496 \) |

Since the above three typical attack types ultimately cause the circuit breaker of this workstation to lose control, the following is the evaluation result of the impact index after the failure of the physical side, as shown in Table 2:

| Name of impact indicator | Importance index of electrical topology | Connectivity rate index | Voltage index | Loss of electricity index |
|--------------------------|----------------------------------------|-------------------------|---------------|--------------------------|
| Impact index evaluation conclusion | \( C^r = 0.031 \) | \( C^q = 0.028 \) | \( C^a = 0.017 \) | \( C^l = 0.0009 \) |

Take the case where the weight of each impact factor of the attack target layer is equal \( \mu_i = 0.25, i \in \{1, 2, 3, 4\} \), the impact factor of the attack at the target level can be obtained \( C'^r = 0.0192 \).

Based on the above results, the risk caused by this attack is finally determined as shown in Table 3:
Table 3. Evaluation results of attack target level impact factor

| Attack event type name | Fuzzing attack | DOS attack | Control permission access attacks |
|------------------------|----------------|------------|----------------------------------|
| Attack incident risk assessment results | $R^\text{path}_{i} = 0.1636$ | $R^\text{path}_{i} = 1.776$ | $R^\text{path}_{i} = 0.1141$ |
| Attack event risk level | III | II | V |

5. Conclusions
Starting with the concept of security assessment, this paper establishes the potential attack path through association algorithm. Considering the attacker's ability, the characteristics of the attack behavior and the characteristics of the target network, the selection probability of the attack path is analysed. According to the two-layer coupled topology model of the target network, the impact factors of the attack action layer and the attack target layer are established from the information side and the physical side, and then the impact degree of the attack on the CPS system is analysed quantitatively, which improves the comprehensiveness and accuracy of the impact consequence analysis of the network attack. Based on the above steps, the risk of the potential attack path is obtained, and then the risk level caused by the attack against the CPS system of the power grid is obtained. Then, the current network attack level is divided by the fuzzy comprehensive evaluation method. Finally, an example is given to analyse the application.

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] 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
[2] 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
[3] 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
[4] Igure V M, Laughter S A, Williams R D 2017 Security issues in SCADA network [J] Computer&security 25(7) 498-506
[5] Ten C, Liu C, Manimaran G 2008 Vulnerability assessment of cybersecurity for SCADA systems [J] IEEE Transactions on power systems 23(4) 1836-1846
[6] Taylor C, Krings A, Alves-foss J 2002 Risk analysis and probabilistic survivability assessment (RAPSA): an assessment approach for power substation hardening[C]// ACM Workshop on Scientific Aspects of Cyber Terrorism, November 21,2002, Washington DC, USA: 9p
[7] NORDSTROM L 2009 Assessment of information security levels in power communication systems using evidential reasoning [J] IEEE Trans on Power Delivery 24(3) 1384-1391
[8] Han Yuqi, Guo Jia, Guo Chuangxin, Huang Han 2016 Intelligent Substation Security Risk Assessment of Cyber Physical Power Systems Incorporating Software Failures [J] Proceedings of the CSEE 36(06) 1500-1508
[9] Li Xin 2017 Research and Implementation of Network Security Assessment Technology Based on Attack Graph [D] Beijing University of Posts and Telecommunications