2024 4th International Conference on Energy, Power and Electrical Engineering (EPEE) | 979-8-3315-1806-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/EPEE63731.2024.10875514

Identification and Prioritization of Critical Transmission Lines Under Malicious Physical Attacks

Keji Chen
Economic and Technical Research Institute
State Grid Zhejiang Electric Power Co., Ltd.
Hangzhou, China

Yingqi Tie*
School of Electrical Engineering
Chongqing University
Chongqing, China
*inget1998@qq.com

Maohua Li
China Electric Power Research Institute
State Grid Corporation of China
Beijing, China

Binrong Zhu
China Electric Power Research Institute
State Grid Corporation of China
Beijing, China

Abstract—**Transmission lines, as essential components for power transmission in the grid, are often exposed to complex external environments, making them vulnerable to malicious physical attacks and natural disasters. Therefore, identifying the criticality of transmission lines and ranking their importance is crucial for enhancing the grid's resilience to such low-frequency but high-impact events. This paper proposes a method to evaluate the importance of transmission lines under malicious attack conditions. This approach is based on an analysis of the attacker's available resources, the most effective attack strategies, and the system operator's re-dispatch actions following an attack. A three-tiered optimization model is formulated to pinpoint the system's most vulnerable transmission lines, with the goal of enhancing their resilience to both physical threats and natural calamities. Furthermore, given the unpredictability of the attacker's behavior, a distributed robust optimization framework is introduced to identify these critical lines under uncertain attack scenarios. To quantify the importance of critical transmission lines in enhancing system resilience to malicious physical attacks, a metric for assessing their criticality is introduced. The effectiveness of the proposed method is validated through its application to the IEEE RTS-79 test system. The results demonstrate that the method effectively identifies and ranks critical transmission lines, improving the grid's ability to withstand potential threats from malicious physical attacks.**

Keywords-transmission lines; importance ranking; malicious physical attacks; criticality index; critical transmission line identification

I. Introduction

As the frequency of extreme events, including physical attacks and natural disasters, continues to rise [1], the concept of a "resilient grid"—capable of resisting and recovering from such disturbances—has gained significant attention [2, 3]. Transmission lines, as key components in power transmission, are frequently exposed to harsh environmental conditions. These include extreme weather events and uncontrollable external forces, which make transmission lines susceptible to faults such as tripping, tower collapse, and line breaks. These failures can lead to power outages, severely impacting electricity supply, daily life, and overall societal development [4, 5]. Therefore, identifying and ranking the importance of transmission lines is crucial for system operators in developing both proactive and reactive response strategies under limited resources, thereby enhancing grid security and reliability.

A significant amount of research has focused on identifying critical components within power grids. For instance, Reference [6] introduced a weighted topological model of the power grid, incorporating the reliability parameters of various components, coupled with structural analysis from complex network theory, providing a method for assessing the vulnerability of critical elements. In [7], an importance index was introduced to identify transmission system components that most affect power system reliability, and reliability-centered maintenance strategies were proposed for key components. Reference [8] introduced a risk-tracking approach to quantify the risk contributions of individual components and identify critical components within the system. Reference [9] developed models for identifying vulnerable transmission lines based on topological parameters and network partitioning, applying complex network theory to power systems. Additionally, [10, 11] proposed methods for identifying critical components under cascading failures, utilizing electrical betweenness as a vulnerability index to effectively detect key elements based on system power flow changes before and after faults. Reference [12] proposed a comprehensive vulnerability assessment system for the grid, incorporating dimensions such as fault probability, load shedding severity, risk levels, and restoration times. Lastly, [13] developed a more complete set of vulnerability indicators for power grids, considering disturbances such as warfare, terrorism, and geological disasters, addressing the needs for both anti-terrorism and disaster prevention in power systems. However, most of the existing research on identifying critical components in power systems has focused primarily on system reliability.

In recent years, the increasing frequency of instability factors such as international terrorism, military conflicts, war threats, and extreme weather events, as highlighted in Reference [14], have emphasized the critical need to bolster the resilience of power systems. Strengthening grid resilience is vital for protecting against both malicious attacks and severe

This work was supported by the Science and Technology Project of State Grid Corporation of China, Grant No. 5200-202319153A-1-1-ZN.

weather conditions, thereby ensuring the safe and stable operation of the power grid, as noted in Reference [15]. Since the concept of grid resilience was introduced, scholars have focused on planning and operational management strategies to improve resilience performance. For example, [16] proposed a resilience enhancement model under typhoon disasters, aiming to minimize system investment and operating costs while maximizing grid resilience, considering measures such as transmission line reinforcement and unit commitment. In [17], the stochasticity and sequential nature of natural disasters were considered, and a Monte Carlo-based approach was used to analyze the potential resilience impacts of extreme weather events, achieving pre-disaster grid prediction. In Reference [18], a cooperative game theory method was introduced to optimize the use of intermittent renewable energy and distributed storage in interconnected microgrids, enhancing system-wide resilience. Likewise, Reference [19] proposed a risk-adaptive islanding defense strategy to facilitate grid recovery during extreme weather events. Reference [20] developed a network topology optimization model designed to increase the resilience of power systems against coordinated cyber-physical attacks.

Notably, identifying critical components of the power system from a resilience perspective can significantly contribute to effective security planning and scheduling in anticipation of potential extreme events. This process provides valuable decision-making support for grid operators. However, most existing research focuses on resilience improvement strategies, with limited studies on identifying critical components within the power system from a resilience-oriented perspective. The identification of critical transmission lines, in particular, has received even less attention. Transmission lines, as vital elements in the power system, operate in complex environments and are highly vulnerable to extreme weather and malicious physical attacks. Such disruptions can lead to serious consequences for both the safe and stable operation of power systems and the broader socio-economic development, as noted in References [21, 22]. To strengthen the resilience of transmission lines against malicious physical attacks, this paper presents a method for identifying critical transmission lines from a resilience perspective, aiming to enhance the system's capability to withstand these threats. By assessing the impact of transmission lines on reducing damage from physical attacks and enhancing grid resilience, the importance ranking of transmission lines is established. This provides grid operators with critical transmission line ranking results, aiding in planning for security investments and scheduling fault recovery processes, thus enhancing the system's resilience to potential physical attacks.

To tackle these challenges, this paper presents a three-layer optimization model that integrates the attacker's resource limitations, optimal attack strategies, and the system operator's response actions to improve grid resilience. Given the uncertainty in the attacker's resources or capabilities, a distributed robust optimization (DRO) model is employed. Furthermore, a criticality index for transmission lines is developed to quantify their significance in enhancing system resilience against malicious physical attacks. The effectiveness of the proposed method is demonstrated through case studies using the IEEE RTS-79 test system. The results confirm that the method accurately identifies and ranks the importance of critical transmission lines under attack conditions. This enhances the grid's ability to withstand potential malicious attacks, providing effective security planning and scheduling for extreme events and supporting decision-making for grid operators.

II. Physical Attack Model of Power Systems

This study focuses on physical attacks targeting power systems, where the attacker seeks to cause maximum disruption by physically damaging transmission lines. If a transmission line is subjected to a physical attack, it is assumed to be disconnected from the grid. As a result, when a physical attack occurs, the affected transmission lines will cease operation. Typically, the system operator responds to an attack by re-dispatching power flows using the optimal power flow (OPF) model to reduce load shedding and lessen the attack's impact. Conversely, the attacker's goal is to maximize total load shedding by anticipating and countering the system operator's optimal dispatch strategies. This dynamic creates a strategic optimization problem, where the attacker seeks to disrupt the power system, while the operator endeavors to minimize the resulting damage.

A. *Objective Function of Physical Attacks on Power Systems*

The primary objective of a physical attack strategy on power systems is to maximize the total load shedding induced by the attack. The attacker's goal is to disrupt the power grid as much as possible, leading to a significant reduction in the system's ability to meet demand. The following objective function is established for this purpose:

$$\max_{\alpha_{i,j}} \sum_{(i,j)\in\varepsilon} L^{*} \tag{1}$$

Where, $\alpha_{i,j}$ represents the physical attack decision for the transmission line between nodes i and j. If the corresponding component is attacked, $\alpha_{i,j}$=1; otherwise, $\alpha_{i,j}$=0. ε is the set of transmission lines in the power grid. L^{*} denotes the amount of load shedding.

B. *Physical Attack Constraints on Power Systems*

Equation (2) represents the resource constraints for physical attack actions.

$$\sum_{(i,j)\in\varepsilon_A} \alpha_{i,j} \le R^{P} \tag{2}$$

where, R^{P} denotes the resource limitations for conducting physical attacks on transmission lines, while ε_A represents the set of transmission lines within the power grid. These constraints ensure that the attacker's resources are taken into account when formulating the attack strategy.

C. *Optimal Re-dispatch Model for Power Systems*

Equations (3) to (8) describe the optimal re-dispatch model utilized by the system's dispatch center following an attack. The main objective, as indicated in Equation (3), is to minimize load shedding. Power flow equations are represented by Equations (4) and (5), while Equations (6) and (7) impose limits on the active power transmission through the lines and the output capacity of the generators. Finally, Equation (8) outlines the constraints on load shedding, determined by the power demand at various nodes.

$$\delta_i^* = \arg\ \min \sum_{i\in N} \delta_i \tag{3}$$

$$p_{i,j} = \frac{v_i - v_j}{x_{i,j}}(1-s_{i,j}),\ \forall (i,j)\in \varepsilon \tag{4}$$

$$\sum_{j\in N:(i,j)\in\varepsilon} p_{i,j} = \sum_{g\in G} p_g - (p_i - \delta_i),\ \forall i \in N \tag{5}$$

$$-p_{i,j}^{\max} \le p_{i,j} \le p_{i,j}^{\max},\ \forall (i,j)\in\varepsilon \tag{6}$$

$$0\le p_g \le p_g^{\max},\ \forall g\in G \tag{7}$$

$$0\le\delta_i\le p_i,\ \forall i\in N \tag{8}$$

where, $p_{i,j}$ represents the active power transmitted between nodes *i* and *j* through the transmission line. $p_{i,j}^{\max}$ denotes the transmission limit of the power flow on the transmission line between nodes *i* and *j*. p_g represents the active power output of generator *g*, while $p_g^{\max}$ indicates the maximum active power output of the generator. v_i / v_j represent the phase angles at bus *i* and bus *j*, respectively. $x_{i.j}$ denotes the reactance of the transmission line between buses *i* and *j*. $s_{i,j}$ is the state variable for the transmission line between buses *i* and *j*. If the transmission line is out of service due to a physical attack, $s_{i,j}$ =1; otherwise, $s_{i,j}$ =0.

III. Identification of Critical Transmission Lines Under Physical Attack Conditions

A. Critical Transmission Line Identification Model

To mitigate the risk of malicious physical attacks on the power grid, system operators can enhance grid resilience by implementing advanced defense technologies, investing in additional security infrastructure, and fortifying transmission line protections. Implementing cost-effective defense strategies that enhance system resilience requires accurately identifying the grid's critical transmission lines. For this purpose, a three-layer optimization model has been developed to pinpoint the most critical lines. A transmission line is deemed critical if its protection significantly reduces the expected load loss in the face of malicious physical attacks. The model for identifying critical transmission lines under such conditions is described as follows:

$$\min_{\zeta_{i,j}} \mathbb{E}\left[\Psi^*\right] = \sum_{\omega\in\Omega} \pi_\omega \Psi_\omega^* \tag{9}$$

$$\text{s.t.} \qquad \sum_{i\in\mathcal{N}} \zeta_{i,j} \le L^{\mathrm{P}} \tag{10}$$

$$\Psi_\omega^* = \arg\max_{\alpha_{i,j,\omega}} \sum_{i\in\mathcal{N}} \delta_{i,\omega}^*, \forall\omega\in\Omega \tag{11}$$

$$\text{s.t.} \qquad \sum_{(i,j)\in\mathcal{E}} \alpha_{i,j,\omega} \le R_\omega^{\mathrm{P}}, \forall \omega\in\Omega \tag{12}$$

$$\delta_{i,\omega}^* = \arg\min \sum_{i\in\mathcal{N}}\delta_{i,\omega}, \forall\omega\in\Omega \tag{13}$$

$$\text{s.t.} \qquad p_{i,j,\omega} = \frac{\vartheta_{i,\omega}-\vartheta_{j,\omega}}{x_{i,j}}\left(1-s_{i,j,\omega}\right) \tag{14}$$

$$\sum_{j\in\mathcal{N}:(i,j)\in\mathcal{E}} p_{i,j,\omega} = \sum_{g\in\mathcal{G}_i} p_{g,\omega} - \left(p_i - \delta_{i,\omega}\right) \tag{15}$$

$$-p_{i,j}^{\max} \le p_{i,j,\omega}\le p_{i,j}^{\max}, \forall(i,j)\in\mathcal{E},\forall\omega\in\Omega \tag{16}$$

$$0\le p_{g,\omega}\le p_g^{\max},\ \ \forall g\in\mathcal{G},\forall\omega\in\Omega \tag{17}$$

$$0\le\delta_{i,\omega}\le p_i,\forall i\in\mathcal{N},\forall\omega\in\Omega \tag{18}$$

The objective function (9) aims to minimize the expected total load loss of the power grid resulting from physical attacks. Expression (10) imposes a constraint on the number of critical transmission lines to be identified. Attack strategies are modeled through expressions (11) – (12), while expressions (13) – (18) describe the system's optimal re-dispatch in response to an attack. The variable $\zeta_{i,j}$ represents whether the transmission line between nodes *i* and *j* is identified as a critical component. If $\zeta_{i,j}$ =1, the transmission line is classified as critical; otherwise, $\zeta_{i,j}$=0. Additionally, when $\zeta_{i,j}$=1, it indicates that the transmission line is protected and therefore not susceptible to physical attacks.

$$s_{i,j,\omega} = \alpha_{i,j,\omega}\left(1-\zeta_{i,j}\right),\ \ \forall(i,j)\in\mathcal{E},\forall\omega\in\Omega \tag{19}$$

Expression (19) represents the status of transmission lines under attack in the power grid, denoted by $s_{i,j,\omega}$. The state of the transmission line between nodes *i* and *j* is independent of the physical attack action $\alpha_{i,j,\omega}$. When $\zeta_{i,j}$=1, even if $\alpha_{i,j,\omega}$=1, the transmission line will not be affected by the physical attack due to the protection it has received. This ensures that the protected transmission lines remain functional despite being targeted by an attack.

B. Robust Optimization Model for Identifying Critical Transmission Lines

In real-world power grids, system operators frequently face difficulties in precisely estimating the distribution of physical attack characteristics. As a result, developing a robust optimization model to identify critical transmission lines becomes crucial for enabling operators to accurately assess their importance and enhance overall system resilience. In contrast to conventional models that assume a precise and known distribution of attacker characteristics for a specific attack scenario, this paper presents a distributed robust optimization model. This model addresses the uncertainty of attack scenarios, which are represented within a bounded fuzzy set $\mathcal{D}$. The formulation of the distributed robust optimization model for identifying critical transmission lines is outlined as follows:

$$\min_{\zeta_{i,j}}\max_{\pi\in\mathcal{D}} \mathbb{E}\left[\Psi^*\right] = \min_{\zeta_{i,j}}\max_{\pi\in\mathcal{D}}\left[\sum_{\omega\in\Omega}\pi_\omega\Psi_\omega^*\right] \tag{20}$$

In this context, π represents the probability distribution within the fuzzy set $\mathcal{D}$, which shares the same distribution characteristics as the historical data, meaning $\pi = \left\{\pi_\omega, \forall\omega\in\Omega\right\}$. Thus, in the distributed robust optimization model, the probability distribution of scenario π_ω transitions from being a fixed parameter, as in the original optimization model, to becoming a variable.

The distributed robust model aims to minimize the expected load loss $\hat{\boldsymbol{\pi}} = \{\hat{\pi}_\omega, \forall \omega \in \Omega\}$ under the worst-case probability distribution, which lies within the defined fuzzy set $\mathcal{D}$. In this study, a norm-based approach is employed to construct the fuzzy set $\mathcal{D}$, and it is formulated as follows:

$$\mathcal{D} = \left\{ \begin{array}{c} \boldsymbol{\pi}(\omega \in \Omega) = 1 \\ \boldsymbol{\pi} \geq \mathbf{0} \\ \| \boldsymbol{\pi} - \hat{\boldsymbol{\pi}} \|_1 \leq \xi_1 \\ \| \boldsymbol{\pi} - \hat{\boldsymbol{\pi}} \|_\infty \leq \xi_\infty \end{array} \right\} \tag{21}$$

where, ξ_1 and ξ_∞ represent the extreme values of the 1-norm and infinity-norm, respectively. The distance between any distribution within the fuzzy set $\mathcal{D}$ and the estimated distribution based on the 1-norm and infinity-norm is constrained by ξ_1 and ξ_∞, respectively.

Therefore, based on the above definitions, the distributed robust optimization model for identifying critical transmission lines is formulated as Equation (20), subject to constraints (21) and (10) – (19). Table I lists the decision variables and objectives in each layer of the multi-level distributed robust optimization problem.

TABLE I. KEY VARIABLES AND OBJECTIVES OF MULTI-LAYER DISTRIBUTED ROBUST OPTIMIZATION PROBLEM

	Decision variable	Objective function
Layer 1	$\zeta_{i,j}, \forall (i,j) \in \mathcal{E}$	$\min \sum_{\omega \in \Omega} \pi_\omega \Psi^*_\omega$
Layer 2	$\pi_\omega, \forall \omega \in \Omega$	$\max \sum_{\omega \in \Omega} \pi_\omega \Psi^*_\omega$
Layer 3	$\alpha_{i,j,\omega}, \forall (i,j) \in \mathcal{E}, \omega \in \Omega$	$\max \Psi^*_\omega, \forall \omega \in \Omega$
Last layer	$\delta_{i,\omega}, \forall i \in \mathcal{N}, \forall \omega \in \Omega$	$\min \Psi^*_\omega, \forall \omega \in \Omega$

C. Solution to the Multi-layer DRO Problem for Identifying Critical Transmission Lines

In the previous section, we introduced the multi-layer DRO model for identifying critical transmission lines. However, this model cannot be directly solved using existing solvers or algorithms. To address this issue, this paper introduces a constraint generation framework that breaks down the original optimization model into a master problem and two distinct subproblems, as shown in Fig. 1.

The first subproblem corresponds to the third and lowest layer of the original model, focusing on determining the most disruptive attack strategy for each scenario while considering the system operator's optimal re-dispatch actions. The second subproblem relates to the second layer of the distributed robust optimization (DRO) model and seeks to identify the worst-case distribution within the fuzzy set Ω. The master problem, representing the top layer of the DRO model, determines the critical transmission lines by integrating the results of both subproblems.

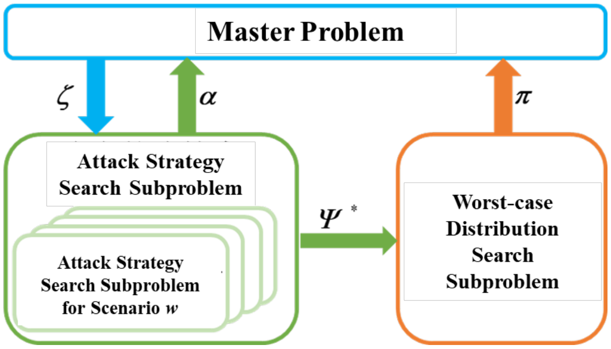
Master Problem
ζ
α
π
Attack Strategy Search Subproblem
Attack Strategy Search Subproblem for Scenario w
Ψ *
Worst-case Distribution Search Subproblem

Figure 1. Master and Sub-Problems for the Solution of the Multi-Level DRO based Models.

In the models for the master problem and subproblems, two distinct subproblems return the attack strategy and the worst-case distribution to the master problem, respectively. The master problem then revises the optimal defense strategy by considering the coordinated attack strategy and the worst-case distribution.

In each iteration of the algorithm, the master problem is solved to obtain the optimal defense strategy, utilizing the attack strategies and probability distributions updated by the subproblems from previous iterations. The first subproblem is then solved to derive the optimal attack strategy, which is based on the newly updated defense strategy. Following this, the second subproblem identifies the worst-case distribution, accounting for both the coordinated attack strategy and the defense solution. These outcomes are then used to refine the attack strategy and the worst-case distribution, which are passed back to the master problem for the subsequent iteration.

IV. EVALUATION OF TRANSMISSION LINE IMPORTANCE

To quantitatively assess the significance of identifying critical transmission lines in enhancing power system resilience, this paper introduces an importance evaluation index for transmission lines. This index facilitates the ranking of transmission lines under conditions of malicious physical attacks.

$$\Lambda_{i,j} = \frac{\sum_{\omega \in \Omega} \sum_{i' \in \mathcal{N}} \left(\pi^*_{\omega| \ \zeta_{i,j}=0} \delta^*_{i',\omega| \ \zeta_{i,j}=0} - \pi^*_\omega \delta^*_{i',\omega} \right)}{\sum_{\omega \in \Omega} \sum_{i' \in \mathcal{N}} \pi^*_\omega \delta^*_{i',\omega}} \tag{22}$$

where $\Lambda_{i,j}$ is the importance index of the transmission line between nodes i and j; π^*_ω and $\delta^*_{i',\omega}$ represent the worst-case probability distribution in scenario ω and the load loss at node i', respectively; $\delta^*_{i',\omega| \ \zeta_{i,j}=0}$ denotes the load loss at node i' due to insufficient protection of the transmission line between nodes i and j; and $\pi^*_{\omega| \ \zeta_{i,j}} = 0$ is the probability of the worst-case scenario ω in the fuzzy set $\mathcal{D}$, where the transmission line between nodes i and j is insufficiently protected.

This index indicates that if the corresponding transmission line is not adequately protected and becomes susceptible to malicious physical attacks, the expected load loss of the grid will increase. A higher importance index signifies that the corresponding transmission line is more critical to the system's recovery capability. Therefore, transmission lines with higher importance levels should be prioritized when planning for system security enhancements and investment strategies.

V. Case Study Analysis

A. Case Description

To verify the performance of the proposed methods for identifying critical transmission lines and evaluating their importance, a case study is conducted using the IEEE RTS-79 system [23]. The connection diagram of the test system is shown in Fig. 2.

In this case study, it is assumed that the upper limit of physical attack resources R^P follows a Beta-binomial distribution. Therefore, for the estimated marginal distribution in the simulation, R^P ~B(3，10，20). The upper bounds for the 1-norm and infinity-norm of the fuzzy sets ξ_1 and ξ_∞ are set to 0.1 and 0.05, respectively.

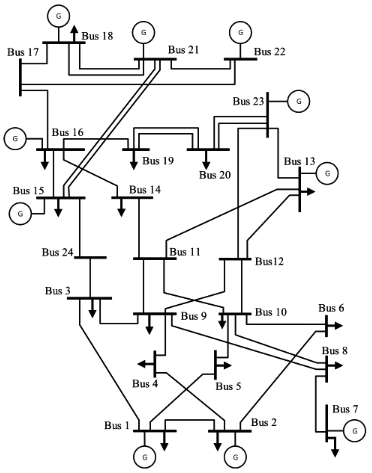

Figure 2. IEEE RTS-79 system single line diagram

B. Analysis of Transmission Line Importance Evaluation

When the number of critical transmission lines to be identified is set to N=8, the proposed model for identifying critical lines under malicious physical attack scenarios identified the following transmission lines as the most vulnerable in terms of attack risk: Line 3-24, Line 7-8, Line 12-23, Line 14-16, Line 15-24, Line 16-17, and Line 17-22. Fig. 3 presents the ranking of transmission lines with the highest importance indices within the test system, while Table II provides the expected load loss for the grid when these critical lines remain unprotected, along with their respective importance indices.

Using the method proposed in this paper, it is possible to accurately identify the critical transmission lines in the grid. If these lines are not adequately protected, they will result in higher load losses under malicious physical attacks. Among all transmission lines, Line 16-17 has the highest importance index. If this line is not protected, it would lead to approximately 600 MW of load loss during a malicious physical attack, which is about 64.45 MW more than the scenario where Line 16-17 is well-protected against attacks. Line 14-16 and Line 12-23 fall in the second tier of importance, with load loss increments of 40 MW and 34 MW, respectively, if unprotected compared to protected lines under attack. Lines 7-8 and 17-22 rank in the third tier, with load loss increments of 21 MW and 18 MW, respectively.

Enhancing the reliability and security of these high-importance transmission lines is critical to ensuring the safe and reliable operation of the system. Strengthening these lines can significantly improve the grid's resilience and ability to withstand potential physical attacks.

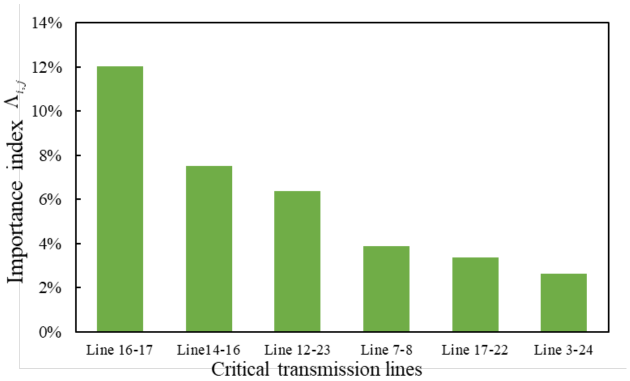

Figure 3. Criticality ranking of transmission lines against Cyber-Physical attacks

TABLE II. Expected Load Loss And Importance Index of Transmission Lines

Lines	Load loss (MW)	Importance index
16-17	599.72	12.04%
14-16	575.57	7.53%
12-23	569.35	6.37%
7-8	556.04	3.88%
17-22	553.32	3.37%
3-24	549.30	2.62%
15-24	549.30	2.62%

C. Analysis of the Impact of L^P on the Importance Evaluation Results of Transmission Lines

Fig. 4 presents the results of critical transmission line identification and importance ranking for different values of L^P . From the figure, it is clear that the identification of critical transmission lines remains consistent across different L^P values, with Line 16-17 consistently ranked as the most critical transmission line, holding the top tier of importance.

In the proposed critical transmission line identification optimization model, when L^P =4, meaning four critical transmission lines are to be identified, the model yields two distinct solutions. The first solution includes Line 16-17, Line 14-16, Line 12-23, and Line 7-8, while the second solution comprises Line 16-17, Line 14-16, Line 12-23, and Line 17-22. In the case where L^P =4, Fig. 4 displays only three critical transmission lines because protecting either Line 7-8 or Line 17-22 has the same impact on the system. When neither of these transmission lines is adequately protected, the expected load shedding is identical, regardless of which line is attacked.

As a result, the same protection effect can be achieved by safeguarding other transmission lines. Hence, when L^P =4, neither Line 7-8 nor Line 17-22 is displayed in the figure. When L^P =6 and L^P =8, the results in the figure are similar to those observed when L^P =4.

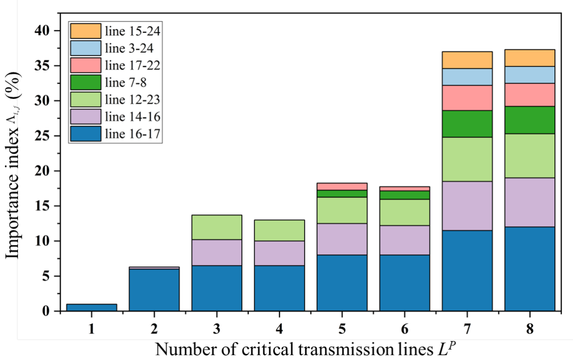

Figure 4. Importance index $\Lambda_{i,j}$ of critical lines with different values of L^P

VI. Conclusion

This paper presents a method for identifying critical transmission lines to evaluate their role in improving the power grid's resilience against malicious physical attacks. A three-tiered optimization model is introduced, which considers the attacker's resource constraints, optimal strategies, and the system operator's response actions, all aimed at enhancing the grid's defenses against potential attacks. In addition, a Distributed Robust Optimization (DRO) model is introduced to address uncertainties regarding the distribution of the attacker's resources and capabilities. To solve this multi-layer DRO model, a constraint generation algorithm is proposed.

An importance index is presented to quantify the significance of transmission lines in protecting the system from malicious physical attacks. The case study analysis demonstrates that the proposed critical transmission line identification method effectively measures the importance of transmission lines within the system in terms of enhancing the grid's resilience to attacks. The method ranks the transmission lines according to their contribution in minimizing the expected load loss from malicious attacks. This approach provides system operators with a robust decision-making tool for protecting critical transmission lines, helping to safeguard the grid from potential malicious attacks.

References

[1] Xue Yusheng, Xiao Shijie. Integrated defense against high risk and small probability events: reflections on power outages and nuclear leakage caused by successive natural disasters in Japan[J]. Automation of Electric Power Systems, 2011, 35(08): 1-11.

[2] Bruneau M, Chang S E, Eguchi R T, et al. A framework to quantitatively assess and enhance the seismic resilience of communities[J]. Earthquake spectra, 2003, 19(4): 733-752.

[3] Li Ning, Andro, Zhang Shiqian, et al. Research Progress and Prospects of Key Technologies for Elastic Power Grids[J]. Electrical Measurement & Instrumentation, 2024, 61(01): 8-16.

[4] Ni Yufan, Zheng Zhanghua, Feng Limin, et al. Insights from Recent Severe Blackouts Abroad for Building a New Power System in China[J]. Electrical Appliances and Energy Efficiency Management Technology, 2023, (05): 1-8.

[5] Lu Yinjun, Li Yijia, Jiang Jinjie, et al. Statistical Analysis of Transmission Line Faults and Research on Prevention and Control Strategies[J]. Shandong Electric Power Technology, 2021, 48(04): 47-52.

[6] Wei Zhenbo, Liu Junyong, Zhu Guojun, et al. Power grid vulnerability assessment model based on reliability weighted topology model[J]. Transactions of China Electrotechnical Society, 2010, 25(08): 131-137.

[7] Pan Yukai, Yu Wenhao, Tang Zhen, et al. Evaluation of Network Node Importance Based on Unit Attributes for Dynamic Reconfiguration[J]. Modern Defense Technology, 2024, 1-13.

[8] Yang Gaofeng, Hu Wen, Fang Qin, et al. Efficient Reliability Evaluation and Weak Link Identification Methods for High Proportion New Energy Power Systems[J]. Advanced Technology of Electrical Engineering and Energy, 2024, 43(04): 43-52.

[9] Jiang Xiong, Chen Chao, Yao Yuhao, et al. Identification of Vulnerable Lines in Power Systems Based on Line Importance Differentiation[J]. Automation & Instrumentation, 2024, (07): 172-175.

[10] Ding Liang, Huang Jianyang, Xu En, et al. Comprehensive Vulnerability Assessment and Structural Optimization Analysis of Power Grid Lines Considering Complex Environmental Characteristics[J]. Power System Protection and Control, 2021, 49(13): 105-113.

[11] Zhang Xiangliang, Lv Feipeng, Zhang Xiangjun, et al. Multi-group cobase minimum breakpoint set selection method considering the number of electrical interfaces of nodes[J]. China Power, 2012, 45(06): 10-13.

[12] Huang Xiaogan, Zhang Yanhui, Yang Bochao, et al. Vulnerability Analysis and Quantitative Evaluation of Power Grids with Wind Power Integration[J]. Power Capacitor & Reactive Power Compensation, 2023, 44(06): 108-116.

[13] Wang Wei, Zhu Jiang, Wei Xingshen, et al. Cybersecurity Vulnerability Assessment for New Distribution Systems[J]. Electric Power Information and Communication Technology, 2024, 22(08): 37-44.

[14] Panteli M, Trakas D N, Mancarella P, et al. Power Systems Resilience Assessment: Hardening and Smart Operational Enhancement Strategies[J]. Proceedings of the IEEE, 2017, 105(99): 1202-1213.

[15] Wang Y, Chen C, Wang J. Research on resilience of power systems under natural disasters-a review[J]. IEEE Transactions on Power Systems, 2015, 31(2): 1-10.

[16] Liu Xiaohang, Chen Jianan, Li Zian. Elastic evaluation of power system considering chain failure under typhoon disaster[J]. Jilin Electric Power, 2023, 51(06): 27-30.

[17] Li Yajing. Research on power system scheduling and elasticity improvement under extreme weather events[D]. South China University of Technology, 2020.

[18] Hammad E. Resilient Cooperative Microgrid Networks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 1539-1548.

[19] Panteli M, Trakas D N, Mancarella P, et al. Boosting the Power Grid Resilience to Extreme Weather Events Using Defensive Islanding[J]. IEEE Transactions on Smart Grid, 2016: 1-10.

[20] Liu Z, Wang L. Leveraging Network Topology Optimization to Strengthen Power Grid Resilience Against Cyber-Physical Attacks[J]. IEEE Transactions on Smart Grid, 2021, 12(2): 1552-1564.

[21] He H, Yan J. Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey[J]. IET Cyber-Physical Systems: Theory & Applications, 2016, 1(1): 13-27.

[22] Karangelos E, Wehenkel L. Cyber-physical risk modeling with imperfect cyber-attackers[J]. Electric Power Systems Research, 2022, 211: 108437.

[23] Reliability Test System Task Force of the Application of Probability Methods Subcommittee, “IEEE reliability test system,” IEEE Trans. Power Appar. Syst., vol. PAS-98, no. 6, pp. 2047–2054, 1979.