Defense Strategy Against Cyber Attacks on Substations Considering Attack Resource Uncertainty

Tianlei Zang, *Senior Member*, *IEEE*, Yujian Xiao, Yunfei Liu, Shijun Wang, Zi'an Wang, and Yi Zhou

***Abstract*—With the rapid integration of communication and information technology into substations, the risk of cyber attacks has significantly increased. Attackers may infiltrate substation networks, manipulate switches, and disrupt power lines, potentially causing severe damage to the power system. To minimize such risks, this paper proposes a three-layer defender-attacker-defender (DAD) model for optimally allocating limited defensive resources to substations. To model the uncertainty surrounding the knowledge of defender of potential attacks in real-world scenarios, we employ a fuzzy analytic hierarchy process combined with the decision-making trial and evaluation laboratory (FAHP-DEMATEL). This method accounts for the attack resource uncertainty by utilizing intelligence data on factors potentially influenced by attackers, which serves as an evaluation metric to simulate the likelihood of various attack scenarios. These uncertainty probabilities are then incorporated into the substation DAD model consisting three layers of agents: the decision-maker, the attacker, and the operator. The decision-maker devises a defense strategy before the attack, while the attacker aims to identify the strategy that causes the maximum load loss. Meanwhile, the operator seeks to minimize the load loss through optimal power flow scheduling. To solve the model, the original problem is transformed into a two-layer subproblem and a single-layer master problem, which are solved iteratively using a column-and-constraint generation algorithm. Case studies conducted on the IEEE RTS-96 system and the IEEE 118-node system demonstrate the effectiveness and practicality of the proposed model. Comparative experiments further highlight the advantages of the proposed model.**

***Index Terms*—Substation, cyber attack, fuzzy analytic hierarchy, decision-making trial and evaluation, defender-attacker-defender, uncertainty, attack resource.**

I. Introduction

GIVEN the widespread adoption of advanced communication and information technologies, power systems are increasingly evolving into cyber physical power systems [1]. The rapid implementation of various control and communication devices within substations has heightened the risk of cyber attacks [2], [3]. Attackers may employ different types of attacks to compromise the security of the power system. Among these, denial-of-service (DoS) attacks [4] and data manipulation attacks [5] are particularly concerning. In DoS attacks, attackers overwhelm the target system with a flood of fake requests, preventing it from processing legitimate ones, leading to communication disruptions and potential service outages within the power system. In data manipulation attacks, attackers alter or falsify data within the system, interfering with the normal operation and decision-making processes. These attacks allow intruders to maliciously infiltrate the cyber domain of substations and unlawfully gain control privileges [6]. They may then issue tripping commands to disconnect critical lines [7], resulting in substantial damage and losses to the system, which poses a significant threat to system security.

In the cyber attack on the Ukrainian power grid in 2015, attackers spent six months conducting internal reconnaissance, including gathering system information through network scanning and social engineering. To understand the network topology and monitor software before launching the attack [8], these efforts ensure that the attackers are well-prepared to exploit the system vulnerabilities effectively. During this incident, the attackers infiltrated the substation networks and used intelligent electronic device (IED) connections to open circuit breakers, resulting in widespread power outage lasting several hours [9]. Therefore, this paper argues that the attacker may have complete knowledge of the system. Just one year later, another transmission substation situated in the capital city of Kyiv, Ukraine, fell victim to a hacker network assault, causing power disruptions that affected one-fifth of the city's population [10]. As substations are one critical part of power infrastructure, they are likely to face an increasing number of cyber attacks in the future. Therefore, safeguarding the cyber security of substations is of utmost importance.

Manuscript received: April 7, 2024; revised: August 3, 2024; accepted: December 2, 2024. Date of CrossCheck: December 2, 2024. Date of online publication: January 20, 2025.

This work was supported by National Natural Science Foundation of China (No. 52377115).

T. Zang, Y. Xiao, Y. Liu, S. Wang, Z. Wang, and Y. Zhou (corresponding author) are with the College of Electrical Engineering, Sichuan University, Chengdu 610065, China (e-mail: zangtianlei@126.com; xyj2228978861@163.com; liuyunfeii@stu. scu. edu. cn; shijunW9312@163. com; wangzianpower@126. com; zhouyipower@163.com).

DOI: 10.35833/MPCE.2024.000375

Traditional power systems apply the $N-1$ criterion to ensure the secure operation of the power grid [11]. However, during actual attacks, attackers often target multiple facilities simultaneously, making reliance on the $N-1$ criterion insufficient to protect the power system from malicious attacks that can damage multiple components at once. To address this limitation, [12] introduces the classic defender-attacker-defender (DAD) model, designed for the strategic allocation of defense resources to minimize load loss resulting from attacks. In practical applications, the information available to defenders about attackers (particularly the quantity of attack resources) is uncertain and difficult to determine accurately. As a result, [13] extends the traditional DAD model to accommodate multiple attack scenarios to reduce attack-induced damage. However, these studies primarily focus on the protection of transmission lines and do not address substation defense. To fill this gap, [14] and [15] propose a bi-level optimization defense model and a three-level DAD model, respectively, for substation defense resource allocation. However, these models do not consider the uncertainty of attack resources in substation defense.

To address the growing complexity of cyber attacks, it is essential to account for the inherent uncertainty. Consequently, this paper incorporates the concept of uncertain attack resources into the substation DAD model. The analytic hierarchy process (AHP) is widely used in various fields for complex decision-making tasks due to its intuitive simplicity and ability to handle qualitative data [16]. However, AHP faces several challenges when dealing with intricate real-world situations. Experts using the 1-9 ratio scales for pairwise comparisons are often constrained by personal experience and limited information, making it difficult to assign precise values [17]. To address these challenges, the fuzzy analytic hierarchy process (FAHP) is introduced [18]. Relying solely on FAHP may overlook the interactions between elements at the same level, which can compromise the accuracy of assessments. To solve this issue, we integrate the decision-making trial and evaluation laboratory (DEMATEL) method [19], which helps mitigate the shortcomings of FAHP. Thus, this paper uses a method that integrates FAHP with DEMATEL to more comprehensively and accurately capture the uncertainty, establishing a substation DAD model adaptable to uncertain attack scenarios and exploring how defenders can formulate optimal defense strategies when the number of substations under potential attack is uncertain.

The main contributions of this paper are summarized as follows.

1) We apply the FAHP-DEMATEL method to model the uncertainty of attack resources, considering the impact of the attacker's skill level, target importance, and other factors on the likelihood of different attack scenarios.

2) We propose a substation DAD model adapted to uncertain attack scenarios, which is designed to cope with a wide variety of cyber attacks. By incorporating the uncertainty, the proposed model is capable of handling both single and multiple attack scenarios.

3) We employ a column-and-constraint generation (C&CG) algorithm to solve the proposed model. The model is divided into the main problem and subproblems. Through iteration, the optimal defense strategy and the minimal load loss are derived. Comparative experiments demonstrate the advantages of the proposed model.

This paper is structured as follows. Section II presents the model establishment. Section III details the solution method. Section IV presents the case study. Section V concludes the discussion and suggests directions for future research.

II. Model Establishment

The modeling process of the proposed model is shown in Fig. 1.

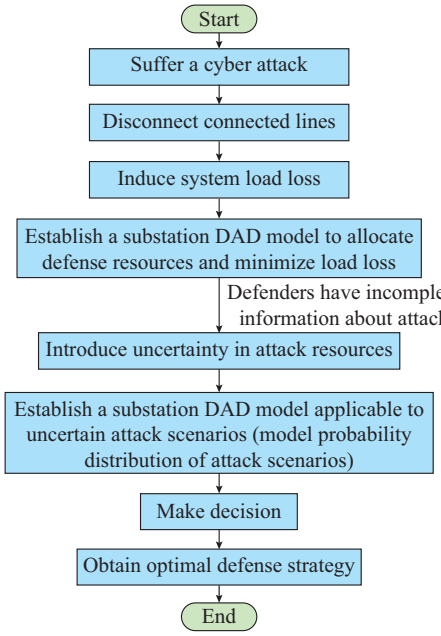

Fig. 1. Modelling process of proposed model.

A. Uncertainty Characterization

In the real world, there is uncertainty regarding the number of targets that attackers may choose to disrupt. Due to challenges defenders face in obtaining accurate information about attackers, decision-making for defense strategies is inherently uncertain.

This uncertainty is represented as a probability distribution over a set of attack resources, where each uncertainty set contains multiple potential attack scenarios, each assigned corresponding probabilities. Possible attack scenarios are influenced by criterion-level indicator such as technical level of the attacker, target importance, time constraint, and defense deployment. Intelligence agencies can gather relevant information about attackers and receive early warnings about potential attacks, enabling security personnel to estimate the number of targets that attackers are likely to to disrupt.

To assess the probability of each attack scenario and construct an uncertainty set, this paper adopts FAHP-DEMATEL method. Under the proposed FAHP-DEMATEL method, defense decisions are based on criterion-level indicators, with information provided by intelligence units. Initially, FAHP is applied to determine a preliminary weight order of the crite-

rion-level indicators. Next, experts adjust the centrality of the indicators by considering their interdependencies and applying the DEMATEL to calculate their centrality. This adjustment yields the final weights for the criterion-level indicators, influenced by the combination of FAHP and DEMATEL. Ultimately, the probability distribution of the attack scenario is derived by integrating the weighted order of the hierarchy elements. The hierarchical structure of applying the FAHP-DEMATEL method to assess the probabilities of attack scenarios is illustrated in Fig. 2. Due to the limitations of the $N-1$ criterion, the minimum number of substations an attacker can choose to attack is 2.

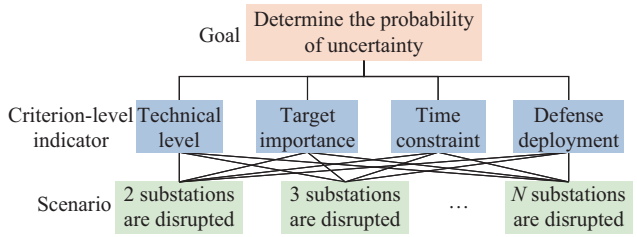

Fig. 2. Hierarchical structure of applying FAHP-DEMATEL method.

The specific uncertainty modeling calculations are as follows.

1) Construct the priority relationship matrix $\boldsymbol{X}=(x_{ij})_{n\times n}$.

Assume that a series of indicators $x_1, x_2, \ldots, x_n$ belong to $\boldsymbol{X}$, $\boldsymbol{X}$ can be expressed as:

$$\boldsymbol{X}=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix} \tag{1a}$$

$$x_{ij}=\begin{cases} 1 & x_i \text{ is more important than } x_j \\ 0.5 & x_i \text{ is as important as } x_j \\ 0 & x_j \text{ is more important than } x_i \end{cases} \tag{1b}$$

where x_{ij} is the indicator representing the degree of relative importance of the former over the latter in a two-by-two comparison of hierarchy $\boldsymbol{X}$, indicator x_i and indicator x_j. In this paper, we use the three-scaled method of 0, 0.5, and 1, as shown in (1b), for comparing the relative importance of indicators to each other.

Defenders measure the relative importance between indicators based on information obtained from intelligence agencies to determine the value of x_{ij}.

2) Convert fuzzy priority matrix to fuzzy consistency matrix $\boldsymbol{Y}=(y_{ij})_{n\times n}$:

$$y_{ij}=\frac{r_i-c_j}{2n}+0.5 \quad i,j=1,2,\ldots,n \tag{1c}$$

where $r_i=\sum_j x_{ij}\,(i=1,2,\ldots,n)$ is the value of the summation by columns in row i of $\boldsymbol{X}$; $c_j=\sum_i x_{ij}\,(j=1,2,\ldots,n)$ is the value of the summation by rows in column j of $\boldsymbol{X}$; and y_{ij} is the element in $\boldsymbol{Y}$.

3) Calculate the initial weights for each indicator in the guideline layer:

$$v_i=\frac{1}{n}-\frac{1}{2\mu}+\frac{1}{n\mu}\sum_j y_{ij} \tag{1d}$$

where μ is the indicator factor for the difference in importance of element y_i and element y_j, and in this paper, we take $\mu=0.5(n-1)$; and v_i is the weight of the indicators of the criterion layer.

4) The defense experts construct a direct impact matrix $\boldsymbol{D}$ based on the degree of interaction between indicators at the guideline level.

The integers from 0 to 4 represent no impact (0), low impact (1), medium impact (2), high impact (3), and very high impact (4), aiming to quantify the magnitude of the impact relationship between the indicators. The direct impact matrix $\boldsymbol{D}=(d_{ij})_{n\times n}$ is established for each level of indicators.

5) Standardize the direct impact matrix and calculate the composite impact matrix $\boldsymbol{Z}$:

$$\boldsymbol{S}=\boldsymbol{D}\Big/\max_{1\le i\le n}\sum_{j=1}^{n} d_{ij}=(s_{ij})_{n\times n} \tag{1e}$$

$$\boldsymbol{Z}=\boldsymbol{S}+\boldsymbol{S}^2+\ldots+\boldsymbol{S}^n=(z_{ij})_{n\times n} \tag{1f}$$

where $\boldsymbol{S}$ is the standardized direct impact matrix; s_{ij} is the element in the i^{th} row and j^{th} column of matrix $\boldsymbol{S}$; $\boldsymbol{Z}$ is the composite impact matrix; and z_{ij} is the magnitude of the impact factor of the i^{th} indicator on the j^{th} indicator.

6) Calculate the indicator centrality h_i.

The indicator centrality reflects the position and importance of the indicator in the indicator system, and is calculated by:

$$h_i=\sum_{i=1}^{n} z_{ij}+\sum_{j=1}^{n} z_{ji} \tag{1g}$$

7) The initial weights of the criterion layer indicators are corrected using h_i to obtain the combined impact weights c of the criterion layer indicators:

$$c=\frac{v_i h_i}{\sum_{i=1}^{n} v_i h_i} \tag{1h}$$

8) Construct the scenario layer priority matrix $\boldsymbol{Q}^r$ under each indicator in the criterion layer separately:

$$\boldsymbol{Q}^r=\begin{bmatrix} q_{11}^r & q_{12}^r & \cdots & q_{1m}^r \\ q_{21}^r & q_{22}^r & \cdots & q_{2m}^r \\ \vdots & \vdots & & \vdots \\ q_{m1}^r & q_{m2}^r & \cdots & q_{mm}^r \end{bmatrix} \tag{1i}$$

where the subscript m indicates the number of elements in the scenario layer. There are n indicators in the criterion layer, so a total of n prioritized relationship matrices needs to be constructed. The respective weight v_i is calculated from each prioritized relationship matrix to synthesize the decision matrix $\boldsymbol{v}=[v_1, v_2, \ldots, v_i, \ldots, v_n]$.

9) Calculate the scenario layer weight (probability distribution of attack scenarios):

$$\boldsymbol{\omega}=\boldsymbol{v}\boldsymbol{c}=\left[v_1, v_2, \ldots, v_i, \ldots, v_n\right]\boldsymbol{c} \tag{1j}$$

where $\boldsymbol{c}$ is the combined impact weights of the criterion-layer indicators.

The corresponding computation process is shown in Fig. 3. This study incorporates the previously mentioned uncertainty set probability distribution into the conventional substation

DAD model to estimate the expected load loss across a range of attack scenarios. The aim is to assist security personnel in minimizing the anticipated load loss of the system during an attack by evaluating a broad range of potential attack scenarios, rather than focusing exclusively on a single attack scenario.

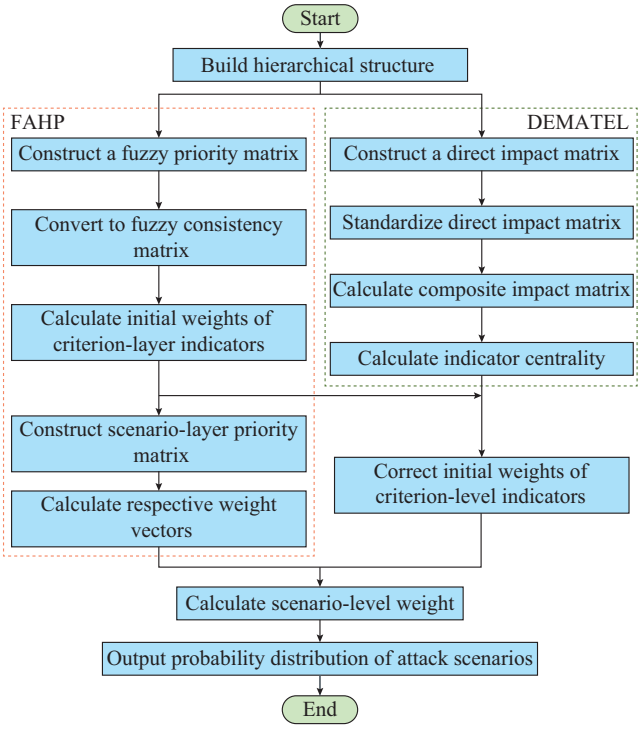

Fig. 3. Computation process of FAHP-DEMATEL method.

B. Substation DAD Model Adaptable to Uncertain Attack Scenarios

The substation DAD model adaptable to uncertain attack scenarios is shown in Fig. 4. This model comprises three hierarchical layers of agents: upper-level decision-makers, middle-level attackers, and lower-level operators. The sequence of actions begins with decision-makers taking the first step to protect several critical substations. The decision on which substations to protect considers both the uncertainty of attack resources and the potential responses of attackers and operators. Following the selection of critical substations for protection by security personnel, attackers initiate attacks by choosing which substations and their connected lines to target for destruction. The attackers' decisions are influenced by the defense strategies of decision-makers and the operation scheduling by the operators. When an attack causes a substation to shut down and a line to be disconnected, operators implement appropriate power flow adjustments to minimize the load loss resulting from the attack.

Unlike traditional models, the proposed substation DAD model does not focus on a single attack scenario. Instead, it introduces uncertainty sets, each containing multiple possible attack scenarios. Upper-level decision-makers engage with numerous middle-level attackers, with the objective of reducing load loss from substation attacks by evaluating all potential attack scenarios and their corresponding probabilities.

The mathematical formulation of the proposed substation DAD model adaptable to uncertain attack scenarios is:

$$\min_{z_n}\left\{\sum_s \omega_s \max_{v_n^s,w_l^s,u_l^s} \min_{P_g^s,f_l^s,\theta^s,\Delta D_d^s}\left\{\sum_d \Delta D_d^s\right\}\right\} \tag{2a}$$

s.t.

$$\sum_n z_n \le R_1 \tag{2b}$$

$$\sum_n v_n \le R_2 \tag{2c}$$

$$\sum_n v_n^s \le \sum_l w_l^s \le K_2 \quad \forall s \tag{2d}$$

$$\sum_{l\in neighbor(n)} w_l^s \ge v_n^s \quad \forall n,\forall s \tag{2e}$$

$$\sum_{l\in neighbor(l)} w_l^s \ge v_{n=o(l)}^s + v_{n=d(l)}^s \quad \forall l,\forall s \tag{2f}$$

$$w_l^s \le v_{n=o(l)}^s + v_{n=d(l)}^s \quad \forall l,\forall s \tag{2g}$$

$$1-u_n^s = v_n^s(1-z_n) \quad \forall n,\forall s \tag{2h}$$

$$u_l^s = w_l^s(1-u_{n=o(l)}^s u_{n=d(l)}^s) \quad \forall l,\forall s \tag{2i}$$

$$f_l^s = -(1-u_l^s)b_l\sum_n K_{L,n,l}\theta_n^s \quad \forall l,\forall s \tag{2j}$$

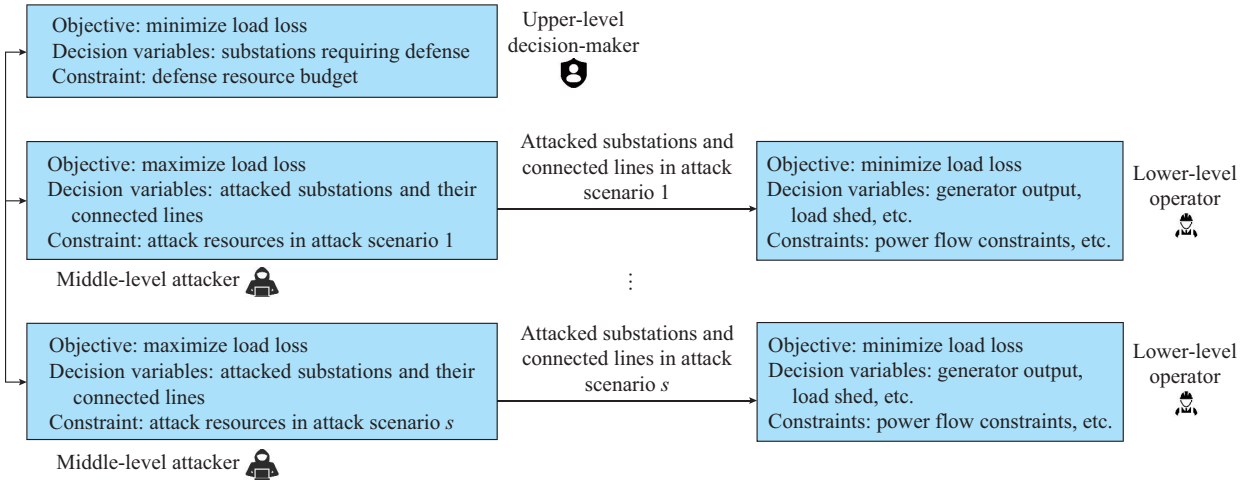

Fig. 4. Substation DAD model adaptable to uncertain attack scenarios.

$$\boldsymbol{K}_L f_l^s = \boldsymbol{K}_P P_g^s - \boldsymbol{K}_D (D_d - \Delta D_d^s) \quad \forall s \tag{2k}$$

$$P_{g,\min} \le P_g^s \le P_{g,\max} \quad \forall g, \forall s \tag{2l}$$

$$-f_{l,\max} \le f_l^s \le f_{l,\max} \quad \forall l, \forall s \tag{2m}$$

$$0 \le \Delta D_d^s \le D_d \quad \forall d, \forall s \tag{2n}$$

$$\theta_{n,\min} \le \theta_n^s \le \theta_{n,\max} \quad \forall n, \forall s \tag{2o}$$

where s is the index for attack scenarios; ω_s is the occurring probability; g is the index of generator; d is the index of load; $o(l)$ is the origin bus of line l; $d(l)$ is the destination bus of line l; *neighbor*(n) is the line connected to substation at bus n; *neighbor*(l) is the line connected to substation at line l; z_n is the binary variable, and $z_n = 1(0)$ indicates that the substation at bus n is hardened (is not hardened); v_n^s is the binary variable, and $v_n^s = 1(0)$ indicates that substation at bus n is under attack (is not under attack); u_n^s is the binary variable, and $u_n^s = 1(0)$ indicates that substation at bus n works normally (works abnormally); w_l^s is the binary variable, and $w_l^s = 1(0)$ indicates that line l is under attack (is not under attack); u_l^s is the binary variable, and $u_l^s = 1(0)$ indicates that line l works normally (works abnormally); P_g^s is the power output of generator g; f_l is the power flow of line l; ΔD_d^s is the load shedding at load d; θ_n^s is the voltage angle at bus n; R_1 is the defense resource budget; R_2 is the substation attack resource budget; K_2 is the line attack resource budget; b_l is the line admittance; $\boldsymbol{K}_L$ is the bus-branch incidence matrix; $\boldsymbol{K}_P$ is the bus-generator incidence matrix; $\boldsymbol{K}_D$ is the bus-load incidence matrix; $P_{g,\min}$ and $P_{g,\max}$ are the lower and upper limits of power output of generator g, respectively; $f_{l,\max}$ is the normal flow rating of line l; D_d is the demand of load d; and $\theta_{n,\min}$ and $\theta_{n,\max}$ are the lower and upper bounds of voltage phase angle, respectively.

The objective function (2a) indicates the expected load loss considering uncertainty. Constraint (2b) represents the limitation on defense resources. Constraint (2c) limits the number of substations that attackers can compromise based on the allocated attack budget. Constraint (2d) caps the number of lines that attackers can disrupt, determined by the line attack budget. Constraint (2e) ensures that if attackers successfully infiltrate a substation, they must disconnect at least one line connected to that substation. Constraints (2f) and (2g) imply that if both substations at the ends of a line are attacked, rational attackers would not target the same line. Constraint (2h) ensures that if a substation is defended, it remains operational and resilient to attacks. Constraint (2i) states that if both substations at the ends of a line are operational, the line remains operational; otherwise, the status of the line depends on the intentions of the attackers. Constraint (2j) represents line flow constraint, typically described using DC optimal power flow models to minimize load shedding behavior in power systems. Constraint (2k) represents power balance constraint. Constraints (2l) - (2o) represent generator output, line flow, load shedding, and power angle constraints, respectively. Constraints (2e) - (2o) incorporate the decisions made by attackers and operators into the decisions on defense strategy from decision-makers. These decisions are based on optimal power flow analysis for each possible attack scenario.

III. Solution Method

This section describes the solution method for the proposed substation DAD model, which is tailored for scenarios with uncertain attack resources. By utilizing the C&CG algorithm, the model is divided into a master problem and several subproblems. The master problem enables decision-makers to evaluate various attack scenarios and formulate defense strategies, considering all possible attack plans. It aims to identify the lower bound (*LB*) of the proposed substation DAD model. In contrast, each subproblem corresponds to an individual attack scenario, facilitating collaborative efforts between attackers and operators in devising optimal attack strategies. Non-converging attack plans are aggregated, enhancing the compilation of expected load losses across all scenarios, thereby establishing the upper bound (*UB*) of the proposed substation DAD model. Iteratively, new variables and constraints are generated and integrated into the master problem. The iterative solution process continues within the framework of C&CG algorithm until the gap between the *UB* and *LB* narrows to a predefined threshold, signifying the acquisition of an optimal defense strategy.

A. Subproblem

In each subproblem, the strategy that inflicts the maximum damage is identified based on a predefined defense method $\hat{\boldsymbol{z}}$. Notably, the model incorporates various sets of uncertainties for attack scenarios, assigning a distinct subproblem to each. During the k^{th} iteration, the specific subproblem addressing attack scenario s is:

$$\max_{v_n^s, w_l^s, u_l^s} \min_{P_g^s, f_l^s, \theta_d^s, \Delta D_d^s} \left\{ \sum_d \Delta D_d^s \right\} \tag{3a}$$

s.t.

$$\sum_n v_n \le R_2 \tag{3b}$$

$$\sum_n v_n^{s,k} \le \sum_l w_l^{s,k} \le K_2 \tag{3c}$$

$$\sum_{l \in neighbor(n)} w_l^{s,k} \ge v_n^{s,k} \quad \forall n \tag{3d}$$

$$\sum_{l \in neighbor(l)} w_l^{s,k} \ge v_{n=o(l)}^{s,k} + v_{n=d(l)}^{s,k} \quad \forall l \tag{3e}$$

$$w_l^{s,k} \le v_{n=o(l)}^{s,k} + v_{n=d(l)}^{s,k} \quad \forall l \tag{3f}$$

$$1 - u_n^{s,k} = v_n^{s,k} (1 - \hat{z}_n) \quad \forall n \tag{3g}$$

$$u_l^{s,k} = w_l^{s,k} (1 - u_{n=o(l)}^{s,k} u_{n=d(l)}^{s,k}) \quad \forall l \tag{3h}$$

$$f_l^{s,k} = -(1 - u_l^{s,k}) b_l \sum_n KL_{n,l} \theta_n^{s,k} \quad \forall l \tag{3i}$$

$$\boldsymbol{K}_L f_l^{s,k} = \boldsymbol{K}_P P_g^{s,k} - \boldsymbol{K}_D (D_d - \Delta D_d^{s,k}) \tag{3j}$$

$$P_{g,\min} \le P_g^{s,k} \le P_{g,\max} \quad \forall g \tag{3k}$$

$$-f_{l,\max} \le f_l^{s,k} \le f_{l,\max} \quad \forall l \tag{3l}$$

$$0 \le \Delta D_d^{s,k} \le D_d \quad \forall d \tag{3m}$$

$$\theta_{n,\min} \le \theta_n^{s,k} \le \theta_{n,\max} \quad \forall n \tag{3n}$$

In (3i), there exists a nonlinear term $u_l^{s,k}\theta_n^{s,k}$. Linearizing it using the Big-M method [20] yields:

$$\begin{cases} f_l^{s,k} - b_l \sum_n KL_{n,l}\theta_n^{s,k} \le M u_l^{s,k} & \forall l \\ b_l \sum_n KL_{n,l}\theta_n^{s,k} - f_l^{s,k} \le M u_l^{s,k} & \forall l \\ -f_{l,\max}(1-u_l^{s,k}) \le f_l^{s,k} \le f_{l,\max}(1-u_l^{s,k}) & \forall l \end{cases} \tag{3o}$$

where $KL_{n,l}$ is the element in the n^{th} row and l^{th} column of matrix $\boldsymbol{K}_L$; and M represents a sufficiently large number.

The two-level max-min programming model is transformed into a corresponding single-level mixed-integer linear programming (MILP) format based on the strong duality theory of linear programming [21].

$$\begin{aligned} \max \Bigg\{ & \sum_n \lambda_n^{s,k} \Bigg(\sum_d KD_{n,d} D_d \Bigg) - \sum_d \gamma_d^{+,s,k} D_d + \sum_g \kappa_g^{-,s,k} P_{g,\min} - \\ & \sum_g \kappa_g^{+,s,k} P_{g,\max} - \sum_l (\xi_l^{+,s,k} + \xi_l^{-,s,k}) f_{l,\max} - \\ & \sum_n (\psi_n^{+,s,k} \theta_{n,\max} - \psi_n^{-,s,k} \theta_{n,\min}) \Bigg\} \end{aligned} \tag{4a}$$

$$\sum_n (KL_{n,l}\lambda_n^{s,k}) + \xi_l^{+,s,k} - \xi_l^{-,s,k} + \mu_l^{s,k} = 0 \quad \forall l \tag{4b}$$

$$\sum_n (KP_{n,g}\lambda_n^{s,k}) - \kappa_g^{+,s,k} + \kappa_g^{-,s,k} = 0 \quad \forall g \tag{4c}$$

$$\sum_n (KD_{n,d}\lambda_n^{s,k}) - \gamma_d^{+,s,k} + \gamma_d^{-,s,k} = 1 \quad \forall d \tag{4d}$$

$$\sum_l \mu_l^{s,k}(1-u_l^{s,k}) b_l KL_{n,l} + \psi_n^{+,s,k} - \psi_n^{-,s,k} = 0 \quad \forall n \tag{4e}$$

$$\xi_l^{+,s}, \xi_l^{-,s}, \kappa_g^{+,s}, \kappa_g^{-,s}, \gamma_d^{+,s}, \gamma_d^{-,s}, \psi_n^{+,s}, \psi_n^{-,s} \ge 0 \tag{4f}$$

where $KD_{n,d}$ is the element in the n^{th} row and d^{th} column of matrix $\boldsymbol{K}_D$; $KP_{n,g}$ is the element in the n^{th} row and g^{th} column of matrix $\boldsymbol{K}_P$; μ_l, λ_n, κ_g, ξ_l, γ_d, and ψ_n are the dual variables for (3i), (3j), (3k), (3l), (3m), and (3n), respectively; and the superscripts + and – are used to distinguish between two dual variables.

The nonlinear term $\mu_l^{s,k}u_l^{s,k}$ in (4e) is linearized using the Big-M method. The nonlinear term $w_l^{s,k}u_{n=o(l)}^{s,k}u_{n=d(l)}^{s,k}$ in (3h) is linearized as:

$$\begin{cases} r_n^{s,k} = w_l^{s,k}u_{n=o(l)}^{s,k}u_{n=d(l)}^{s,k} \\ r_n^{s,k} \le w_l^{s,k} \\ r_n^{s,k} \le u_{n=o(l)}^{s,k} \\ r_n^{s,k} \le u_{n=d(l)}^{s,k} \\ r_n^{s,k} \le w_l^{s,k} + u_{n=o(l)}^{s,k} + u_{n=d(l)}^{s,k} - 2 \end{cases} \tag{4g}$$

where $r_n^{s,k}$ is an auxiliary variable.

After solving the subproblem corresponding to attack scenario s, the maximum load shedding value Q_s and the attack plan $\hat{v}_n^{s,k+1}, \hat{w}_l^{s,k+1}$ are obtained. Additionally, in the k^{th} iteration, a set of additional scheduling variables ($P^{s,k+1}$, $f^{s,k+1}, \theta^{s,k+1}, \Delta D^{s,k+1}$) and their associated constraints are obtained, which are then added to the master problem.

B. Master Problem

The objective of the master problem is to determine the lower bound solution and formulate a safeguarding strategy for viable solutions, termed upper bound solutions. With the assumption that K iterations are completed, the master problem is outlined as:

$$\min_{z_n} \left\{ \sum_s \omega_s \pi_s \right\} \tag{5a}$$

s.t.

$$\sum_n z_n \le R_1 \tag{5b}$$

$$\pi_s \ge \sum_d \Delta D_d^s \quad \forall s, k = 1, 2, \ldots, K \tag{5c}$$

$$1 - u_n^{s,k} = \hat{v}_n^{s,k}(1 - z_n) \quad \forall n, \forall s, k = 1, 2, \ldots, K \tag{5d}$$

$$u_l^{s,k} = \hat{w}_l^{s,k}(1 - u_{n=o(l)}^{s,k} u_{n=d(l)}^{s,k}) \quad \forall l, \forall s, k = 1, 2, \ldots, K \tag{5e}$$

$$f_l^{s,k} = -(1-u_l^{s,k}) b_l \sum_n KL_{n,l}\theta_n^{s,k} \quad \forall l, \forall s, k = 1, 2, \ldots, K \tag{5f}$$

$$\boldsymbol{K}_L \boldsymbol{f}_l^{s,k} = \boldsymbol{K}_P \boldsymbol{P}_g^{s,k} - \boldsymbol{K}_D (\boldsymbol{D}_d - \Delta \boldsymbol{D}_d^{s,k}) \quad \forall s, k = 1, 2, \ldots, K \tag{5g}$$

$$P_{g,\min} \le P_g^{s,k} \le P_{g,\max} \quad \forall g, \forall s, k = 1, 2, \ldots, K \tag{5h}$$

$$-f_{l,\max} \le f_l^{s,k} \le f_{l,\max} \quad \forall l, \forall s, k = 1, 2, \ldots, K \tag{5i}$$

$$0 \le \Delta D_d^{s,k} \le D_d \quad \forall d, \forall s, k = 1, 2, \ldots, K \tag{5j}$$

$$\theta_{n,\min} \le \theta_n^{s,k} \le \theta_{n,\max} \quad \forall n, \forall s, k = 1, 2, \ldots, K \tag{5k}$$

$$\begin{cases} r_m^{s,k} = u_{n=o(l)}^{s,k} u_{n=d(l)}^{s,k} & \forall l, \forall s, k = 1, 2, \ldots, K \\ r_m^{s,k} \le u_{n=o(l)}^{s,k} & \forall l, \forall s, k = 1, 2, \ldots, K \\ r_m^{s,k} \le u_{n=d(l)}^{s,k} & \forall l, \forall s, k = 1, 2, \ldots, K \\ r_m^{s,k} = u_{n=o(l)}^{s,k} + u_{n=d(l)}^{s,k} - 1 & \forall l, \forall s, k = 1, 2, \ldots, K \end{cases} \tag{5l}$$

where $r_m^{s,k}$ is an auxiliary variable. The linearization of the non-linear term in (5e) yields (5l).

The non-linear term $u_l^{s,k}\theta_n^{s,k}$ specified in (5f) undergoes linearization through the Big-M method, akin to the method taken in the subproblem.

After obtaining a solution in the k^{th} iteration of the master problem, we acquire the optimal defense strategy z_n^{k+1} and the optimal scheduling variables ($P^{s,1}, P^{s,2}, \ldots, P^{s,k}$, $f^{s,1}, f^{s,2}, \ldots, f^{s,k}, \theta^{s,1}, \theta^{s,2}, \ldots, \theta^{s,k}, \Delta D^{s,1}, \Delta D^{s,2}, \ldots, \Delta D^{s,k}$) generated in the subproblem corresponding to attack scenario s, and consequently, pinpoint the optimal values π_s^{k+1} of variables established within the master problem.

C. Overall C&CG Algorithm Solving

The model of substations, adapting to the uncertainty of attack resources, is decomposed into subproblems and master problems. The C&CG algorithm is utilized for analysis. The specific implementation steps of the model solution algorithm are provided below.

Step 1: set $LB = -\infty$, $UB = +\infty$, and initiate the iteration count k to 1. Establish the convergence threshold ε.

Step 2: resolve the master problem (5) to identify the optimal defense strategy z_n^{k+1} and optimal scheduling variables.

Update $LB = \sum_s \omega_s \pi_s^{k+1}$.

Step 3: solve the subproblem (3) corresponding to attack scenario s to obtain the optimal solution $Q_s(z_n^{k+1})$ and the optimal attack plan $\hat{v}_n^{s,k+1}, \hat{w}_l^{s,k+1}$. If the k^{th} iteration completes all subproblems, move to *Step 4*; if not, repeat *Step 3*.

Step 4: update $UB = \min\left\{UB, \sum_s \omega_s Q_s(z_n^{k+1})\right\}$. If $UB - LB \le \varepsilon$, end the process; otherwise, proceed to *Step 5*.

Step 5: introduce new variables $(P^{s,k+1}, f^{s,k+1}, \theta^{s,k+1}, \Delta D^{s,k+1})$, $\forall s$ into the master problem, increase the iteration counter k, and loop back to *Step 2*.

IV. Case Study

This section details case studies performed on the IEEE RTS-96 system [22], encompassing 24 nodes, 12 generators, 17 loads, and 38 lines, and the IEEE 118-node system. The proposed substation DAD model is solved using MATLAB 2021a and the Gurobi 9.5.2 solver. All computations are performed on a personal laptop equipped with an i5-8300H processor, running a 64-bit version of Windows 10, and having 16 GB of RAM. For clarity, we define the number of substations that attackers can attack as attack resources and the number of substations defenders can protect as defense resources. Attack resource uncertainty is modeled through different scenarios, each with its corresponding probability.

A. An Example for FAHP-DEMATEL Method to Model Uncertainty

In this subsection, an example is provided to illustrate how the FAHP-DEMATEL method can be used to model the uncertainty of the attack resources. Firstly, the attack resource is set to be 5. Due to the limitation of the $N-1$ criterion, the number of substations that the attacker can choose to destroy is 2, 3, 4, or 5. There are 4 elements in the scenario layer, and since there are 4 indicators in the criterion layer, it is necessary to construct a 4×4 $\boldsymbol{X}$, a 4×4 $\boldsymbol{D}$, and four 4×4 $\boldsymbol{Q}^r$.

Based on the information received from intelligence agencies, the matrices $\boldsymbol{X}$ and $\boldsymbol{D}$ can be presented as:

$$\boldsymbol{X} = \begin{bmatrix} 0.5 & 0 & 1 & 1 \\ 1 & 0.5 & 1 & 1 \\ 0 & 0 & 0.5 & 1 \\ 0 & 0 & 0 & 0.5 \end{bmatrix} \tag{6}$$

$$\boldsymbol{D} = \begin{bmatrix} 0 & 4 & 3 & 3 \\ 3 & 0 & 3 & 3 \\ 0 & 2 & 0 & 1 \\ 0 & 2 & 0 & 0 \end{bmatrix} \tag{7}$$

$x_{21} = 1$ represents the view of intelligence agencies that the target importance is more important to the attacker than the technical level of the attacker. The initial weights of the criterion layer indicators are calculated as $\boldsymbol{v} = [0.29,\ 0.37,\ 0.21,\ 0.13]^{\mathrm{T}}$, the indicator centrality is calculated as $\boldsymbol{h} = [3.00,\ 3.68,\ 2.11,\ 2.19]$, and the combined impact weight of the criterion-layer indicators is calculated as $\boldsymbol{c} = [0.29,\ 0.46,\ 0.15,\ 0.10]^{\mathrm{T}}$.

Based on the expert analysis of the interactions between the indicators at the guideline level. $\boldsymbol{Q}^r$ can be presented as:

$$\boldsymbol{Q}^1 = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0 \\ 1 & 1 & 0.5 & 0 \\ 1 & 1 & 1 & 0.5 \end{bmatrix} \tag{8}$$

$$\boldsymbol{Q}^2 = \begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 1 & 0.5 & 0.5 & 0 \\ 1 & 0.5 & 0.5 & 0 \\ 1 & 1 & 1 & 0.5 \end{bmatrix} \tag{9}$$

$$\boldsymbol{Q}^3 = \begin{bmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \end{bmatrix} \tag{10}$$

$$\boldsymbol{Q}^4 = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 1 & 0.5 & 0.5 & 0.5 \\ 1 & 0.5 & 0.5 & 0.5 \end{bmatrix} \tag{11}$$

$q_{21} = 0.5$ represents the equal probability that the attacker chooses to attack two substations or three substations, subject only to the technical level of the attacker. The calculation yields $\boldsymbol{v}_1 = [0.17,\ 0.17,\ 0.28,\ 0.38]^{\mathrm{T}}$, $\boldsymbol{v}_2 = [0.13,\ 0.25,\ 0.25,\ 0.37]^{\mathrm{T}}$, $\boldsymbol{v}_3 = [0.25,\ 0.25,\ 0.25,\ 0.25]^{\mathrm{T}}$, $\boldsymbol{v}_4 = [0.17,\ 0.25,\ 0.29,\ 0.29]^{\mathrm{T}}$. The probability distribution of possible attack scenarios is $\boldsymbol{\omega} = [v_1, v_2, \ldots, v_i, \ldots, v_n]$, $\boldsymbol{c} = [0.16,\ 0.23,\ 0.26,\ 0.35]^{\mathrm{T}}$, which means that the probability phase of the attacker choosing to attack 2, 3, 4, and 5 substations in this cyber attack operation is 0.16, 0.23, 0.26, and 0.35, respectively.

B. Impact of Uncertainty in Attack Resources on Protection Strategies

The power grid is frequently targeted by deliberate cyber attacks, where attackers seek to gain unauthorized control over substations by infiltrating the network, enabling them to send false information and disrupt the connected lines. Possible attack scenarios are influenced by factors such as the technical level of the attacker, target importance, time constraint, and defense deployment. These factors lead to varying degrees of uncertainty regarding the execution of malicious actions. This subsection explores the impact of uncertainty in attack resources on decision-making processes of the defender when formulating optimal protection strategies. A range of uncertain scenarios is simulated, e. g., different types of attackers. Utilizing the proposed substation DAD model, we calculate the optimal defense strategies and the minimum load losses under different uncertainties. The resulting minimum load loss represents an expected value, which is the probability-weighted average of load shedding of the system across multiple attack scenarios within a specific uncertainty set.

This subsection simulates the information provided by the intelligence agencies to enable the defenders to model seven different types of attackers, corresponding to seven uncertainty probability sets (UPSs) labeled as attackers 1-7. The attack resource R_2 is set to be 5 and the defense resource R_1 is set to be 3. The defenders estimate the number of substations the attackers may target to be 2, 3, 4, or 5 (correspond-

ing to attack scenarios 1, 2, 3, 4) with different probabilities. For example, the UPS [0.16, 0.23, 0.26, 0.35] indicates that the probability of attackers targeting 2 substations is 0.16, 3 substations is 0.23, 4 substations is 0.26, and 5 substations is 0.35. The objective of the decision-makers among the defenders is to minimize load loss from attacks while prioritizing the defense of three substations. The simulation results for this UPS are presented in Table I.

TABLE I
SIMULATION RESULTS FOR UPS [0.16, 0.23, 0.26, 0.35]

Variable	Result
Expected load loss (MW)	417
Defended substation	9, 11, 12
Load loss in attack scenario 1 (MW)	138
Load loss in attack scenario 2 (MW)	221
Load loss in attack scenario 3 (MW)	415
Load loss in attack scenario 4 (MW)	677

As shown in Fig. 5, the uncertainty in probabilities significantly influences the decision-making of defense strategies. For attacker 1 (with UPS as [1, 0, 0, 0], and the subsequent UPSs correspond to attackers 2-7), the defense anticipates that this attacker will only target two substations, representing a scenario without uncertainty in attack resources, i.e., a single attack scenario. In this case, the optimal defense strategy is to protect substations 14, 16, and 19 to reduce the load loss from attacks.

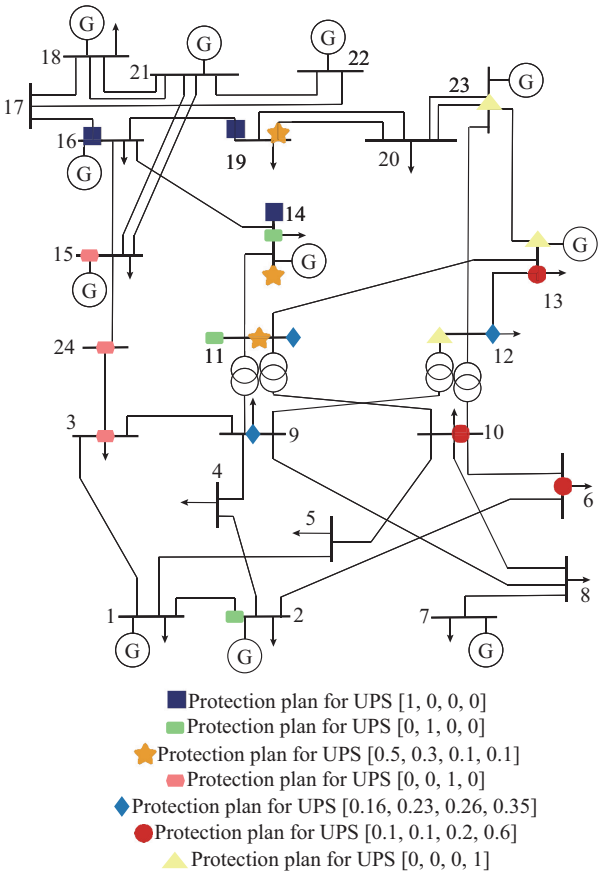

Fig. 5. Protection plan for $R_1 = 3$ and $N_s = 5$.

For attacker 3, the defense estimates that the probabilities that the attacker will target two, three, and four or five substations are 50%, 30%, and 10%, respectively. Therefore, the defense must consider the possibility of attacks on two or three substations more extensively, while not disregarding the chance of four or five substations being attacked, despite their lower probabilities. Compared with the potential single attack scenario posed by attacker 1, dealing with attack resource uncertainty requires more complex decision-making and scheduling for the defense. Considering the four potential attack scenarios and their corresponding probabilities, the defense concludes that protecting substations 11, 14, and 19 is the most effective strategy for reducing the anticipated load loss resulting from attack.

For attacker 5, the defense estimates that the probabilities that the attacker will target two, three, four, and five substations are 0.16, 0.23, 0.26, and 0.35, respectively. As a result, the defender must consider a broader range of possible attack scenarios involving different numbers of substations. Dealing with the attack resource uncertainty demands more complex decision-making and scheduling by the defense than the single-attack scenario posed by attacker 1. Considering the four potential attack scenarios and their corresponding probabilities, protecting substations 9, 11, and 12 is identified as the most effective strategy to minimize expected load loss resulting from the attack.

For attacker 6, the defense should pay more attention to the possibility of the attacker targeting five substations. Thus, the defense strategy is to protect substations 6, 10, and 13.

Figure 6 shows that the expected load loss increases as the number of substations targeted by the attacker increases. Specifically, with a probability distribution of [0.5, 0.3, 0.1, 0.1] suggesting a high likelihood of two or three substations being attacked, the proposed substation DAD model predicts the minimum expected load loss of 266 MW. Conversely, when the probability distribution shifts to [0.1, 0.1, 0.2, 0.6], indicating a higher probability of attacking five substations, results in a substantial increase in the minimum expected load loss to 578 MW. Moreover, a probability distribution of [0, 0, 0, 1], which signifies an assured attack on five substations, raises the minimum expected load loss to 638 MW, reflecting an increase of 60 MW in system damage compared with a scenario with a 60% chance of targeting five substations.

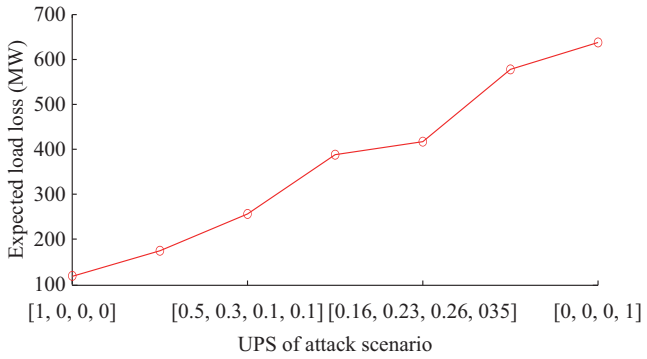

Fig. 6. Expected load loss for various attack scenarios.

C. Impact of Defense Resources on Protection Strategies and Load Loss

In this subsection, with the attack resources being fixed at 5, the attacker can also choose to attack 2, 3, 4, or 5 substations. We adjust the defense resources between 3 and 5 to examine the influence of defense resource availability on protection strategies amidst uncertain attack resources. Figure 7 illustrates the results of load loss under different defense resource allocations for the seven UPSs. As can be observed from Fig. 7, in each attack scenario, when defense resources increase, the damage suffered by the system is mitigated, resulting in a lower load loss.

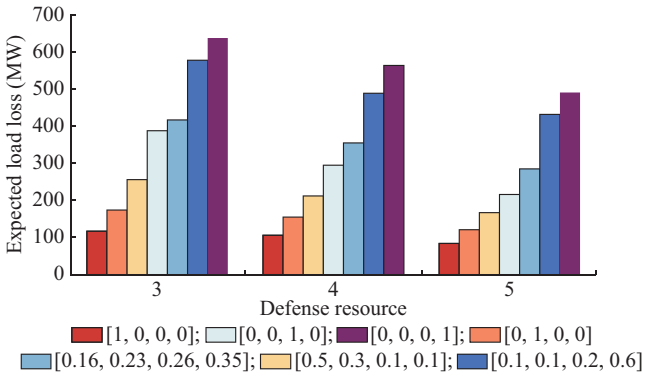

Fig. 7. Results of load loss under different defense resource allocations for seven UPSs.

Here are the specific simulation results for three UPSs, corresponding to attacker 3 [0.5, 0.3, 0.1, 0.1], attacker 5 [0.16, 0.23, 0.26, 0.35], and attacker 6 [0.1, 0.1, 0.2, 0.6]. These results explore the optimal protection strategies and the minimum load losses in different defense resource scenarios. The serial number of defended substations and the expected load losses, corresponding to the increase in defense resources for the three UPSs, are detailed in Tables II, III, and IV.

TABLE II
DEFENSE PERFORMANCE OF DIFFERENT DEFENSE RESOURCES FOR UPS [0.5, 0.3, 0.1, 0.1]

R_1	Defended substation	Expected load loss (MW)
3	11, 14, 19	256
4	11, 14, 16, 19	212
5	26, 14, 16, 19	167

TABLE III
DEFENSE PERFORMANCE OF DIFFERENT DEFENSE RESOURCES FOR UPS [0.16, 0.23, 0.26, 0.35]

R_1	Defended substation	Expected load loss (MW)
3	9, 11, 12	417
4	9, 11, 12, 13	355
5	9, 10, 11, 14, 16	285

The results indicate that with an increase in defense resources, more substations are protected, leading to a reduction in expected load loss. If more substations can be protected under the assumption of known attack resources, the impact of attacks on the system will be further minimized.

TABLE IV
DEFENSE PERFORMANCE OF DIFFERENT DEFENSE RESOURCES FOR UPS [0.1, 0.1, 0.2, 0.6]

R_1	Defended substation	Expected load loss (MW)
3	6, 10, 13	578
4	6, 10, 13, 23	489
5	3, 12, 13, 23, 24	432

Furthermore, the selection of protected substations is not random. Under specific UPS of attack scenarios, certain substations are primary targets for attackers. Once attacked, these substations would result in significant load loss. Taking the case of defending against attacker 3 as an example, as defense resources gradually increase, substations 9 and 11 remain key sites for system protection in the subsequently derived optimal protection plans for the same attack scenario.

Specifically, when defense resources increase from 3 to 5 in defending against attacker 3, the system can protect two additional substations in the same attack scenario, resulting in a reduction of 102 MW in expected load loss.

D. Comparison with Models Without Considering Uncertainty

To illustrate the benefits of the proposed substation DAD model adapted to uncertain attack scenarios, this subsection conducts a comparative study with the traditional model. The uncertainty scenario of attacker 5 is chosen for analysis.

In the traditional model, with attack resources set to be 5, if defenders only consider attack scenario 1 and attackers will target two substations, the optimal defense strategy (denoting the defended substations) obtained is [14, 16, 19]. If defenders only consider attack scenario 2 and attackers will target three substations, the optimal defense strategy is [2, 11, 14]. If defenders only consider attack scenario 3 and attackers will target four substations, the optimal defense strategy is [3, 15, 24]. If defenders only consider attack scenario 4 and attackers will target five substations, the defense strategy obtained is [12, 13, 23]. However, if the proposed substation DAD model considers the the attack resource uncertainty represented by defense UPS [0.16, 0.23, 0.26, 0.35], the optimal defense strategy derived is to protect substations 9, 11, and 12, as shown in Table I. Tables V-VIII describe the effects of each defense strategy applied to scenarios 1, 2, 3, and 4, respectively, and present the corresponding expected load loss.

These strategies are compared with those derived from that considering only single-attack scenario, applied to the load losses of each scenario and total expectations. Tables V-VIII and Fig. 8 reveal that the defense strategy [9, 11, 12] based on the optimization model that accounts for attack resource uncertainty does not always lead to the lowest load loss for specific attack scenarios. However, when considering the total expectation of load losses across multiple attack scenarios, it proves to be the most efficient strategy.

TABLE V
SIMULATION RESULTS FOR UPS [1, 0, 0, 0]

Variable	Result
Optimal defense strategy	[14, 16, 19]
Expected load loss at defense UPS (MW)	435
Load loss in attack scenario 1 (MW)	117
Load loss in attack scenario 2 (MW)	251
Load loss in attack scenario 3 (MW)	441
Load loss in attack scenario 4 (MW)	697

TABLE VI
SIMULATION RESULTS FOR UPS [0, 1, 0, 0]

Variable	Result
Optimal defense strategy	[2, 11, 14]
Expected load loss at defense UPS (MW)	424
Load loss in attack scenario 1 (MW)	152
Load loss in attack scenario 2 (MW)	174
Load loss in attack scenario 3 (MW)	420
Load loss in attack scenario 4 (MW)	716

TABLE VII
SIMULATION RESULTS FOR UPS [0, 0, 1, 0]

Variable	Result
Optimal defense strategy	[3, 15, 24]
Expected load loss at defense UPS (MW)	440
Load loss in attack scenario 1 (MW)	143
Load loss in attack scenario 2 (MW)	281
Load loss in attack scenario 3 (MW)	388
Load loss in attack scenario 4 (MW)	716

TABLE VIII
SIMULATION RESULTS FOR UPS [0, 0, 0, 1]

Variable	Result
Optimal defense strategy	[12, 13, 23]
Expected load loss at defense UPS (MW)	451
Load loss in attack scenario 1 (MW)	130
Load loss in attack scenario 2 (MW)	276
Load loss in attack scenario 3 (MW)	553
Load loss in attack scenario 4 (MW)	638

For instance, the optimal defense strategy [14, 16, 19] obtained by considering only attack scenario 1 results in a minimum load loss of 117 MW when assuming that attackers will target only two substations. However, when attack scenarios 2, 3, and 4 occur (where three, four, and five substations are attacked, respectively), this defense strategy is no longer optimal. Applying this defense strategy to all four attack scenarios yields a total expectation of load loss of 435 MW, higher than 417 MW obtained by considering the attack resource uncertainty and adopting the defense strategy [9, 11, 12]. Similarly, the defense strategy [2, 11, 14], derived from considering only attack scenario 2, results in the minimum load loss of 174 MW when assuming that attackers will target three substations. However, its total expectation of load loss across all scenarios is 424 MW, still higher than 417 MW. The subsequent defense strategies derived from that considering only attack scenarios 3 and 4 yield total expected load losses of 440 MW and 451 MW, respectively.

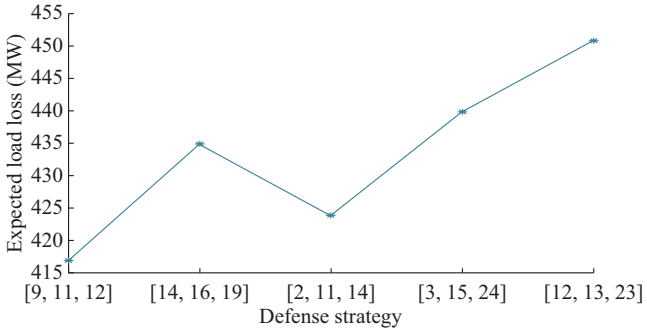

Fig. 8. Expected load loss for each defense strategy at defense UPS [0.16, 0.23, 0.26, 0.35].

Therefore, although traditional substation DAD models can be used to develop optimal defense strategies for defending against a specific single-attack scenario, their defensive performance will be weak when there is attack resource uncertainty. In contrast, the proposed substation DAD model, which considers attack resource uncertainty, is more suitable for real-world applications where multiple attack scenarios need to be considered simultaneously.

E. Performance of Proposed Substation DAD Model in IEEE 118-node System

In order to test the scalability of the proposed substation DAD model and algorithms in large systems, the IEEE 118-node system is used as an example for simulation analysis. The defense UPS [0.16, 0.23, 0.26, 0.35] is still selected as the object of study in this subsection. The simulation results in the IEEE 118-node system are shown in Table IX.

TABLE IX
SIMULATION RESULTS FOR DEFENSE UPS [0.16, 0.23, 0.26, 0.35] IN IEEE 118-NODE SYSTEM

Variable	Result
Expected load loss (MW)	391
Optimal defense strategy	[27, 68, 116]
Load loss in attack scenario 1 (MW)	301
Load loss in attack scenario 2 (MW)	346
Load loss in attack scenario 3 (MW)	380
Load loss in attack scenario 4 (MW)	470

As shown in Table IX, the optimal defense strategy in this attack scenario is [27, 68, 116], with a total expected load loss of 391 MW.

In the test of IEEE 118-node system, when the defender considers that the attacker will target only two substations, the optimal defense strategy is [5, 8, 25]. When the defender assumes that the attacker will target three substations, the op-

timal defense strategy becomes [10, 86, 116]. If the defender anticipates that the attacker will target four substations, the optimal defense strategy is [25, 68, 116]. Furthermore, if the defender assumes that the attacker will target five substations, the obtained defense strategy is [5, 28, 27], as illustrated in Fig. 9.

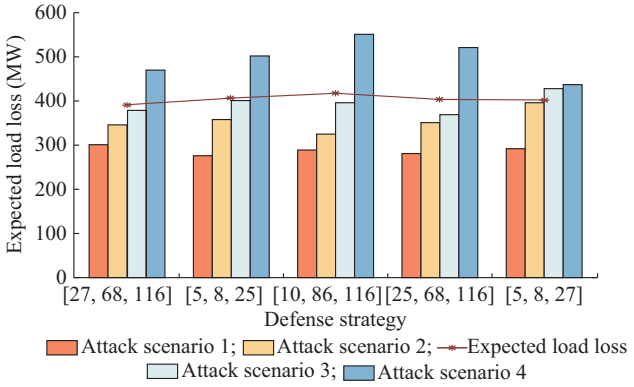

Fig. 9. Defense strategy application scenarios and corresponding load losses.

As shown in Fig. 9, the defense strategy based on the proposed substation DAD model accounts for the attacking resource uncertainty [27, 28, 116]. Although this strategy may not result in the lowest load loss in a specific deterministic attack scenario, it proves to be the most effective when considering multiple potential attack scenarios. The expected load loss under this protection scheme, which addresses uncertainty, is minimized.

Therefore, the proposed substation DAD model remains applicable when large systems encounter attack resource uncertainty.

V. Conclusion

This paper introduces a novel substation DAD model that adapts to attack resource uncertainty. The model expands the traditional framework to integrate the attacker resource uncertainty by using FAHP-DEMATEL method, which accounts for the impact of uncertainty on the decision-making process involving the decision-maker, the attacker, and the defender. The proposed substation DAD model is subsequently reorganized into a main problem and multiple subproblems for unified solution using the C&CG algorithm. Case studies conducted on the IEEE RTS-96 system and IEEE 118-node system explore various UPSs for attack resources, simulating different types of attackers. The main conclusions drawn are as follows.

1) Attack resource uncertainty significantly affects decisions regarding defense strategies of substations. The proposed substation DAD model can address both single-attack scenarios and situations where multiple uncertain attack scenarios may occur, as well as decide on defense strategies that minimize the expected load loss under different UPSs of attack scenarios.

2) With an increase in defense resources, the optimal defense strategy does not change randomly, which can further mitigate the load loss caused by attacks in specific scenarios.

3) Comparative studies illustrate that the defense strategies derived from the proposed substation DAD model may not be optimal for a specific determined attack scenario under uncertain attack information. However, the defense strategy minimizes the expected load loss when considering the probabilities of uncertain attack scenarios comprehensively.

The proposed substation DAD model is based on several assumptions, including the behavior patterns of the attackers, distribution of attack resources, and certainty of system parameters. However, these assumptions may not align perfectly with real-world scenarios, potentially affecting the accuracy and applicability of the proposed substation DAD model. Furthermore, we primarily consider specific types of cyber attack scenarios, while other types of attacks such as insider attacks and physical sabotage are not accounted for in the proposed substation DAD model. These unconsidered attack types may have a significant impact on power systems in real-world situations. To address these limitations and expand the scope of uncertainty and attack scenarios, future research could consider incorporating additional types of uncertainty, such as multi-stage attacks that attackers may launch. Additionally, the proposed substation DAD model could be extended to the defense of microgrids and integrated energy systems.

References

[1] D. Du, M. Zhu, X. Li *et al.*, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727-743, May 2023.

[2] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1035-1044, Feb. 2020.

[3] S. Hussain, S. M. S. Hussain, M. Hemmati *et al.*, "A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems," *Protection and Control of Modern Power Systems*, vol. 8, no. 3, pp. 1-15, Jul. 2023.

[4] W. Chen, D. Ding, H. Dong *et al.*, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1688-1697, Aug. 2019.

[5] P. García-Teodoro, J. Díaz-Verdejo, E. Vázquez *et al.*, "Anomaly-based network intrusion detection: techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1, pp. 18-28, Feb. 2009.

[6] T. Ustun and S. Hussain, "An improved security scheme for IEC 61850 MMS messages in intelligent substation communication networks," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 3, pp. 591-595, May 2020.

[7] M. Ding, X. Li, and J. Zhang, "Effect of SCADA-oriented cyber attack on power system reliability," *Power System Protection and Control*, vol. 46, no. 11, pp. 37-45, Dec. 2018.

[8] S. Roy, N. Sharmin, A. Laszka *et al.*, "Survey and taxonomy of adversarial reconnaissance techniques," *ACM Computing Surveys*, vol. 55, no. 6, pp. 1-38, Jun. 2023.

[9] M. F. Ahern, "Cybersecurity in power systems," *IEEE Potentials*, vol. 36, no. 5, pp. 8-12, Sept. 2017.

[10] T. Patrick. (2016, Dec.). Ukrainian power company "99% certain" blackout result of cyber attack. [Online]. Available: http: //www. defenseone.com/technology/2016/12/ukrainian-power-company-99-certain-blackout-result-cyber-attack/134099/?oref=d-river

[11] M. Zhou, C. Liu, A. Jahromi *et al.*, "Revealing vulnerability of $N-1$ secure power systems to coordinated cyber-physical attacks," *IEEE Transactions on Power Systems*, vol. 38, no. 2, pp. 1044-1057, Mar. 2023.

[12] W. Yuan, L. Zhao, and B. Zeng, "Optimal power grid protection through a defender-attacker-defender model," *Reliability Engineering*

& System Safety, vol. 121, pp. 83-89, Jan. 2014.
[13] Y. Xiang and L. Wang, "An improved defender-attacker-defender model for transmission line defense considering offensive resource uncertainties," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2534-2546, May 2019.
[14] Y. Zhao, Y. Cao, and Y. Li, "Risk-based contingency screening method considering cyber-attacks on substations," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4973-4976, Nov. 2022.
[15] Y. Zhao, Y. Cao, and Y. Li, "A substation-based tri-level model for hardening resource allocation," in *Proceedings of 2021 IEEE 5th Conference on Energy Internet and Energy System Integration*, Taiyuan, China, Aug. 2021, pp. 320-325.
[16] F. Ernest and S. Gass, "The analytic hierarchy process – an exposition," *Operations Research*, vol. 49, no. 4, pp. 469-486, Aug. 2001.
[17] T. Evangelos and S. H. Mann, "Using the analytic hierarchy process for decision making in engineering applications: some challenges," *International Journal of Industrial Engineering: Applications and Practice*, vol. 2, no. 1, pp. 35-44, Feb. 1995.
[18] F. Ahmed and K. Kilic, "Fuzzy analytic hierarchy process: a performance analysis of various algorithms," *Fuzzy Sets and Systems*, vol. 362, no. 1, pp. 110-128, May 2019.
[19] T. Hamed and M. Mitra, "Understanding applications and best practices of DEMATEL: a method for prioritizing key factors in multi-criteria decision-making," *Journal of Management Science & Engineering Research*, vol. 6, no. 2, pp. 17-23, Jul. 2023.
[20] B. Ti, G. Li, J. Wang *et al*., "Identification of critical transmission lines in cyber-physical power system considering monitoring function and control function," *Proceedings of the CSEE*, vol. 42, no. 7, pp. 2556-2566, Jul. 2022.
[21] T. Ding, C. Li, C. Yan *et al*., "A bilevel optimization model for risk assessment and contingency ranking in transmission system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3803-3813, Sept. 2017.
[22] J. Pinheiro, C. Dornellas, M. Schilling *et al*., "Probing the new IEEE reliability test system (RTS-96): HL-II assessment," *IEEE Transactions on Power Systems*, vol. 13, no. 1, pp. 171-176, Sept. 1998.

Tianlei Zang received the B.S., M.S., and Ph.D. degrees in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2009, 2012, and 2017, respectively. From 2017 to 2020, he holds a postdoctoral position with Tsinghua University, Tsinghua, China. He is presently an Associate Professor in the College of Electrical Engineering, Sichuan University, Chengdu, China. His research interests include energy cyber physical system, and operation optimization and safety analysis of integrated energy system.

Yujian Xiao received the B.S. degree in School of Electromechanical and Vehicle Engineering from Chongqing Jiaotong University, Chongqing, China, in 2022, and is currently pursuing the M.S. degree in the College of Electrical Engineering from Sichuan University, Chengdu, China. His research interests include vulnerability assessment and security of new power system.

Yunfei Liu received the B.S. degree in School of Electrical Engineering from Zhengzhou University, Zhengzhou, China, in 2022, and is currently pursuing the M.S. degree in the College of Electrical Engineering from Sichuan University, Chengdu, China. His research interests include distribution network resilience and cyber physical system.

Shijun Wang received the B.S. degree in School of Electrical Engineering and Automation from Shihezi University, Shihezi, China, in 2022, and is currently pursuing the M.S. degree in the College of Electrical Engineering from Sichuan University, Chengdu, China. His research interest includes anomaly detection of cyber physical power system.

Zi'an Wang received the B.S. degree in School of Electrical and Automation Engineering from Nanjing Institute of Technology, Nanjing, China, in 2022, and is currently pursuing the M.S. degree in the College of Electrical Engineering from Sichuan University, Chengdu, China. His research interests include vulnerability assessment and situation awareness of cyber physical power system.

Yi Zhou received the B.S. and Ph.D. degrees in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2016 and 2021, respectively. From 2019 to 2020, he worked as a Visiting Doctoral Scholar with Aalborg University, Aalborg, Denmark. He is currently with Sichuan University, Chengdu, China, as a Post-doctoral Researcher. His research interests include stability analysis and control of power electronic based power system.