Received 2 October 2022, accepted 4 November 2022, date of publication 21 November 2022,
date of current version 30 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223651

RESEARCH ARTICLE

A Novel Four-Level Approach for Improving Power System Resilience Against Intentional Attacks

FARSHAD FARAMARZI[1], TAHER NIKNAM[1], (Member, IEEE), MOTAHAREH POURBEHZADI[2], (Member, IEEE), GITI JAVIDI[2], (Member, IEEE), AND EHSAN SHEYBANI[2], (Senior Member, IEEE)

[1]Department of Electronic and Electrical Engineering, Shiraz University of Technology, Shiraz 71557-13876, Iran
[2]School of Information Systems and Management, Muma College of Business, University of South Florida, Tampa, FL 33620, USA

Corresponding author: Ehsan Sheybani (sheybani@usf.edu)

This work was supported in part by the Interdisciplinary Research Grant (IRG) through the University of South Florida, Sarasota-Manatee Campus.

ABSTRACT This study proposes a new four-level model to enhance the resilience of power systems against human attacks. The model considers human attacks such as intelligent attackers and power system planners as defenders. The attackers want to maximize the impact of actions, while the defender tries to avoid imposed costs and damages due to budget limitations. The classic resilience model is a three-level defense-attack-defense (DAD) model, which includes the hardening measure, human attack, and recovery levels. In this study, power system planning, as a new defensive layer, was added prior to the conventional DAD. The proposed method becomes a four-level defense-defense-attack-defense (DDAD) model. To this end, a new four-level defense-defense-attack-defense (DDAD) model is proposed, in which a new defense layer is added to the common three-level defense-attack-defense (DAD) model. Looking at the model more closely, new power plants and substations are added to the power system to improve its resilience, and the most important power plants and substations are determined. Subsequently, a conventional three-level model was applied. In this research, the defender and attacker have strategies with their own costs for every power system component, such as power plants and substations, and their own interactions. The power system model includes the load, power plant and substation, and substation priority, which are defined as a combination of the values of the load and network topology. The proposed model was applied to the IEEE-30 bus test system, and the results indicated the effectiveness of the proposed method.

INDEX TERMS Four-level resilience model, intentional human attack, power system planning, resilience.

I. INTRODUCTION

A. MOTIVATION

A power system is the infrastructure of a modern economy, and its reliable and safe operation is a requisite for our social life. However, many natural disasters and intentional human attacks have occurred recently in power systems, causing challenging power outages. Resilience is vital for safe and efficient operation of power systems against severe natural or intentional events. In the United States, extreme weather events are the leading cause of many power system outages and annually cost an average of more than 18 billion dollars [1]. However, in recent years, the risk of man-made attacks on power systems has increased. A warning example is the intentional human attack on the Metcalf Transmission Substation in California in 2013 [2]. In a recent report, the Committee on Science and Technology for Countering Terrorism emphasized that a nation's electric power systems must be made more resilient to terrorist attacks [3]. The impact of human attacks on critical infrastructures is greater and more complex than that of other hazards, such as natural disasters [4]. An expert enemy targets the most sensitive equipment of the network that causes the cutoff of the most critical and other loads at the lowest attacker's cost.

The associate editor coordinating the review of this manuscript and approving it for publication was Jahangir Hossain.

Invaders usually have an advantage over defenders because they can choose the element and time of attack [5]. As a result, the increasing resilience of power networks against human attacks is a critical issue in protecting the electrical infrastructure.

1) LITERATURE REVIEW

Several models have been proposed to address this problem. The classic resiliency model, which is a tri-level defender-attacker-defender (DAD) model, is based on finding the best hardening strategy before and after an attack to minimize the influence of attacks. In the first level, defenders select the best strategy to harden the network. At the second level, the attackers disrupted the network in a scenario with maximum damage. At the third level, defenders respond to the attack by the recovery network.

In early works, a bi-level series-parallel model of optimal defense strategy was investigated, assuming that the enemy tries to maximize either the expected damage or the success probability of an attack [6] and [7]. In [8], an infrastructure location and protection problem against multiple noncooperative choice attackers was modeled, and a two-stage stochastic bi-level programming problem was proposed to solve the problem. Motto et al. [9] transformed a mixed-integer bi-level model into a one-level mixed-integer linear model using duality theory, which is more efficient than the previous models. In [10], the authors presented a bi-level attack–defense (AD) framework to determine the critical loads using cascading failure scenarios. Many attack scenarios are generated at the first level. In the second stage, the results are evaluated to determine the critical equipment of the power system for resilience enhancement. However, this model cannot be used for large-scale networks. Therefore, in [11], the authors proposed a decomposition method using the global Benders decomposition algorithm (GBDA) to solve the problems of the previous method. Levitin introduced a model using a universal generating function technique for damage to a complex multistate series – parallel system by human attack [12]. This model suggests a defense strategy assuming that the system components have separate protection methods, the attackers want to maximize the expected damage of an offense, and invaders attack other targets using a similar strategy. Hausken improved the previous model by suggesting a classic series-parallel system in which the elements can be interdependent, interlinked, and independent [13] and [14]. In this model, defender attackers use multiple strategies by merging the reliability theory, operational research, and game theory. In [15], a mixed-integer non-linear programming problem (MINLP) is proposed to determine the critical contingencies caused by different reasons, such as human attacks in a power system. The authors proposed a new solution based on Benders' decomposition within a restart framework. Brown et al. proposed a tri-level defense-attack-defense model to determine the most critical elements of a power system to protect against intentional attack [16]. Yao et al. improved the bi-level model applied in [10] and the tri-level model in [16] by introducing a tri-level optimization model in which defenders can allocate budgets by conducting a sensitive analysis [17]. Brown et al. [16] and Yao et al. [17] agree that creating a tri-level model by adding an extra level of defense to the bi-level model produces a better protection strategy because of the increasing interaction between defenders and attackers. Romero et al. [18] improved the algorithm proposed in [17] by introducing a general tri-level non-linear model. The disadvantages of this approach are that it is time-consuming and complicated because of the nonlinear formulation.

In [19], the equivalent two-stage DAD model was proposed. In this model, a scenario is defined for human attackers who want to disable some elements of a power network with intentional operations, whereas another scenario is defined for defenders who attempt to eliminate or minimize the impact of attacks. The model comprises three stages.

1) Defenders provide circumstances that prevent or minimize the effectiveness of any offensive before an attack (hardening).
2) Attackers attempt to interrupt the service of the power system through intentional actions (attack).
3) Defenders attempt to continue services by recovering the system after attack (recovery).

Yuan et al. improved the tri-level approach for a complex power grid using a column-and-constraint generation (C&CG) method to optimize resource defense planning [20]. The authors developed a previous work using the nested column-and-constraint generation (NC&CG) method by adding line switching and a comprehensive protection algorithm [21]. Consequently, an optimized resource allocation strategy for the defender was determined. Wu et al. improved the technique proposed in [19] using (C&CG) method to solve the suggested model [22]. The authors in [23] introduced a tri-level algorithm that defenders and attackers want to minimize the system operating cost (SOC), which is the cost of load shedding and generator operating cost. In this model, attackers can attack and defenders must defend three basic components in power systems: power plants, transmission lines, and substations. Although most subsequent work has focused on distribution network resiliency against natural disasters, some studies have simultaneously described attacks on several related infrastructures. Schneider et al. investigated the resiliency of the European electricity system and the Internet in a complex network and proposed an algorithm for increasing network resilience in an onion-like structure using the heuristic edge-swap (ES) method [24]. In the following, the attack model proposed in [25] on the two-layer community structure is used to evaluate the resiliency of complex networks and mitigate vulnerability against intentional attacks using the heuristic edge-addition (EA) algorithm. In this model, enemies first attack a small-scale node, and the second invasion is on a large-scale community structure, and enhances resiliency by adding new lines between nodes. Fang et al. enhanced the algorithm in [24] and [25] by adding several structural edges to solve the optimization problem and increase the resiliency of a complex network [26]. The authors applied this method to a complicated system that included three real networks, two general artificial networks, and an improved network resilience against malicious attacks.

In [27], a tri-level DAD algorithm that achieved better resilience performance by determining the weakness of a complex gas-electric network against intentional attacks was proposed. This algorithm has binary variables and uses the nested column-and-constraint generation (NC&CG) method to solve the inner problem. Li et al. improved previous DAD models by hardening vulnerable points against human attacks by adding new elements [28]. The authors used (NC&CG &) & method and applied the proposed algorithm to an electric water system to demonstrate the advantages of this model. In this study, a new model was introduced to improve electric power grid resilience against intentional attacks by adding a new defensive layer to the classic model.

In [29], a bi-level algorithm was proposed, while the power transmission system, battery storage systems, and natural gas system were considered to minimize operation and planning costs. The problem was modeled as a stochastic decomposition method and solved using the (C&CG) algorithm. In [30], a bi-level problem was proposed to optimize the energy market benefits transmitted between distribution and transmission systems [30]. At the first level, the worst-contingency-like human attack in transmission elements is considered, and then unit commitment is carried out to check security limitations. In [31], a method was proposed to increase the resiliency of a gas-electric network by providing operational robustness to the power system in a multistage trapezoidal resilience. In [32], a resilience enhancement method was suggested to improve the resilience of the distribution system against natural disasters. The problem was modeled as a knapsack problem, and a fault tree analysis method was applied to solve it. In [33], the transmission line was a vulnerable component against human attacks, and a four-stage power system planning was proposed to mitigate the negative impacts of the attacks.

2) MAIN CONTRIBUTIONS

This paper proposes a new four-layer defense-defense-attack-defense (DDAD) model in which power system planning is added as an extra layer in the first step. In this study, a new strategy to improve power system resilience against human attacks is proposed by adding a new defensive layer to the classic solution. The methodology can determine load, power plants, and substation priorities, while considering the interaction between defense and attack levels. According to this model, important and vulnerable components of networks are identified, and, with redesign, power system defenders attempt to defend that point. The redesign of the network includes the construction of new power plants or substations at appropriate positions.

The main contributions are as follows:

- A new defensive layer is added to the classic three-level model, leading to the mitigation of the defense cost:
- A great diversity of attack strategies (e.g., either human or equipment attack) from different points of view, such as technical and financial limitations, can be considered as attack scenarios in the proposed method.
- A great diversity of defenders' strategies according to budget and technical limitations can be considered using the proposed method.
- Power system expansion planning, such as new power plants and substations, can be proposed as the first defensive strategy.
- The load priority and value of the electrical equipment are considered at all levels of the proposed method, leading to solving optimization problems.

II. MODEL DESCRIPTION

In this study, a defense-attack scenario was considered for modelling. In this strategy, attackers try to prevent power delivery to loads and defenders want to continue servicing by operating in multiple stages. The proposed models for each layer are explained as follows.

A. PRE-EVALUATION MODEL

The proposed strategy requires an adequate assessment of resiliency before the main stages, which is called a pre-evaluation model. In the pre-evaluation stage, it is predicted that attackers can attack substations or power plants in accordance with their resource and network vulnerabilities before any defense operations in the normal network mode. Then, the value of each substation and power plant from the perspective of the attackers is determined. First, the optimization problem in the third level is formulated; then, the first and second optimization levels are formulated as conjunction problems.

B. FIRST LEVEL (PLANNING MODEL)

In this study, a new defense layer is added to the conventional framework at the first level. This is a hardening planning measure for designing a hardened power network against intentional attacks by adding new power plants and substations. The proposed planning model is different from classic expansion network planning. It is assumed that the power network is sufficient in accordance with the conventional model; however, it is necessary to plan and construct new power plants and substations and minimize the possibility of attacks on critical and other loads in accordance with the values obtained in the pre-evaluation stage. The construction cost of new power plants and substations is the main constraint to this problem.

C. SECOND LEVEL (HARDENING MODEL)

In this step, the vulnerable elements of the power network are determined in the pre-evaluation step, and hardening measures are implemented to improve the resilience of the power network. It is assumed that defenders have several protection methods, and attackers must select an optimal solution to overcome them. In this study, human protection (HP), such as using security guards, and physical protection (PP), such as using reinforced buildings or transferring to underground or withering human protection or physical protection (HPP), are considered hardening measures to protect power plants and substations against intentional attacks. It is assumed that hardening of each power plant or substation has a separate cost with regard to the hardened type. Defenders' resources (e.g., the number of protection groups and protection budget) are restricted. The proposed problem is a multi-objective optimization problem, whose objective function is to minimize the hardening cost and maximize hardened loads with high values in critical loads in the first priority and other loads in the second priority. Power plant and substation values were obtained during the pre-evaluation stage.

D. THIRD LEVEL (ATTACK MODEL)

Attacks on each power plant or substation cause out-of-service elements and outages [20]. It is assumed that the attackers are experts, can access the necessary power system information, and can determine the most vulnerable power plants and substations from the point of resiliency. Therefore, they attack power plants and substations to outage critical loads in the first step, and other loads according to the value of the power plants and substations determined in the pre-evaluation stage in the second step, considering their restrictions. Attackers must prepare a human specialist group and equip them with necessary equipment. Therefore, human and financial resources were the first restrictions imposed by attackers. Attackers can be attacked using a method related to the defence procedure described at the hardening level. Invaders can attack unprotected elements (UA) or use human attacks (HA) or physical attacks (PA), such as using more advanced equipment. In this text, it is assumed that enemies cannot attack elements that are protected by humans and the physical (HPP). The relationship between the defenders' method and the attackers' measures is presented in Table 1.

TABLE 1. Relationship between defenders and attackers' method.

Defenders' method	none	HP	PP	HPP
Attackers' method	UA	HA	PA	none

Therefore, the type of defence determines the type of attack, which is the second restriction. The defender's method for substations is introduced by HPS, PPS, and HPPS, and for power plants, it is shown by HPG, PPG, and HPPG. Attackers'substation methods are introduced by UAS, HAS, and PAS, and power plants are shown by UAG, HAG, and PAG. It is assumed that attacks on each power plant or substation have separate costs with regard to attack type. The main goal of attackers is to impose significant damage, which is inferred to outage maximization, while having a limited budget to attack.

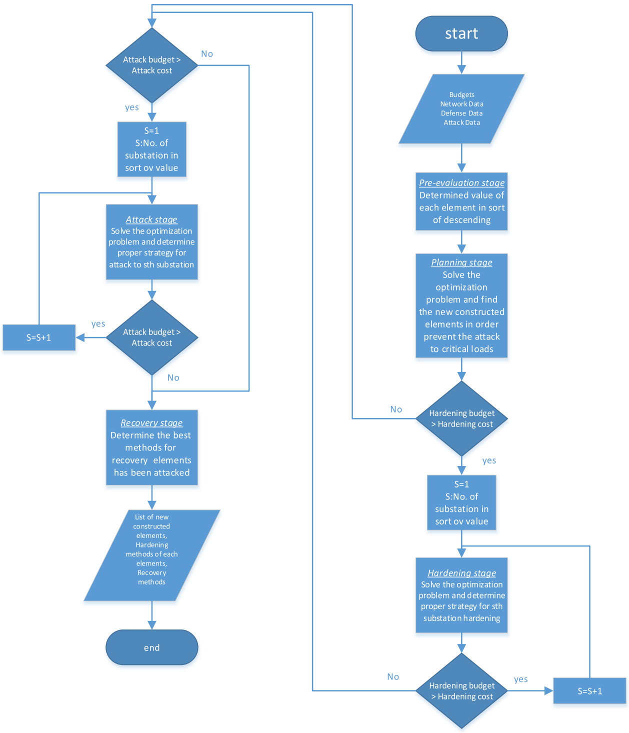
start
Budgets
Network Data
Defense Data
Attack Data
Pre-evaluation stage
Determined value of each element in sort of descending
Planning stage
Solve the optimization problem and find the new constructed elements in order prevent the attack to critical loads
Hardening budget > Hardening cost
No
yes
S=1
S:No. of substation in sort ov value
Hardening stage
Solve the optimization problem and determine proper strategy for sth substation hardening
Hardening budget > Hardening cost
No
yes
S=S+1
Attack budget > Attack cost
No
yes
S=1
S:No. of substation in sort ov value
Attack stage
Solve the optimization problem and determine proper strategy for attack to sth substation
Attack budget > Attack cost
yes
S=S+1
No
Recovery stage
Determine the best methods for recovery elements has been attacked
List of new constructed elements, Hardening methods of each elements, Recovery methods
end

FIGURE 1. Flowchart of general four level model.

E. FORTH LEVEL (RECOVERY MODEL)

This is the last level at which the operator attempts to recover the system after a terrorist attack. It is assumed that the power plants and substations that are attacked will be disconnected from the power network, and the system operator will make an effort to recover the loads with regard to priority. The power system operator may split the network, impose load shedding on maintain substations, or control the reactive power injected by the remaining power plants with an Automatic Voltage Regulator (AVR). to prevent voltage drops in the substations. It should be noted that the process of recovery of critical loads is the first priority, and other loads are the second priority, according to their values.

To make the matter clearer the general flowchart including inputs, procedures, solving method and outputs of the entire four level model is shown in Fig. 1.

III. PROBLEM FORMULATION

In this section, the mathematics of the problem are presented, and a heuristic solution is proposed. Each model described in Section II has a separate mathematical formulation, which is explained as follows:

A. PRE-EVALUATION FORMULATION

At this stage, the effect of the outage for each substation and power plant is determined as follows:

$$ES_s = IC1 \times (\frac{P_d^s}{1000}) \tag{1}$$

$$EG_g = COVD_g \tag{2}$$

In (1), the normalized average load interruption cost for 1 h for different loads for each substation is determined as the effect of the outage for each substation [29]. Another way to interrupt loads is by invading the power plants. Attacks on power plants decrease the voltage of substations with critical loads directly or cause to go lines active or active/reactive power of other generators beyond standard limits, causing out-of-service loads by this secondary effect. In (2), the effect of outage for each power planet is obtained by summing the normalized average load interruption cost for 1 h for different loads due to substations' voltage drops less than 0.95 p.u. with the first and secondary effects. Then, the attacked substations and power plants in accordance with the attackers' resources are predicted in two steps as follows:

Step 1:

Case A:

$$max \sum\nolimits_{h^a} \sum\nolimits_{k} CL_k^{h^a} z_k^{h^{a-pe}} \tag{3}$$

$$min \sum_{h^a} \sum_{k} CCL_k^{h^a} z_k^{h^{a-pe}} \tag{4}$$

Case B:

$$max \sum\nolimits_{e^a} \sum_{g} \sum_{k} VD_k^{e^{a-g}} x_{kg}^{e^{a-pe}} \tag{5}$$

$$min \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{k} CVD_k^{e^{a-g}} x_{kg}^{e^{a-pe}} \tag{6}$$

Case C:

$$max \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{h^a} \sum\nolimits_{k} (CL_k^{h^a} + VD_k^{e_g^a}) xz_{kg}^{eh^{a-pe}} \tag{7}$$

$$min \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{h^a} \sum\nolimits_{k} (CCL_k^{h^a} + CVD_k^{e_g^a}) xz_{kg}^{eh^{a-pe}} \tag{8}$$

In Step 1, the attackers want to cut off the maximum critical loads in accordance with their resources. In case A, the enemies only attack substations with critical loads, case B only attacks power plants, and case C simultaneously attacks substations and power plants. In Case A, a multi objective optimization problem was solved using (3) and (4). In (3), the maximum critical load outage is solved and in (4), the minimum attack cost is considered. Another way to interrupt critical loads is by invading the power plants. For this purpose, the multi objective optimization problem in Case B was solved. In (5), the maximum critical loads with a voltage drop of less than 0.95 p.u. are solved, while in (6), the minimum attack cost is determined. In case C, a multi objective optimization problem is solved in (7) and (8), which invaders attack substations with critical loads and power plants simultaneously. In step 2, with the remaining budget, the enemies attack another load in accordance with the following equations in step 2.

Step 2:

Case A:

$$\max \sum_{f^a} \sum_{s} ES_s y_s^{f^{a-pe}} \tag{9}$$

$$\min \sum_{f^a} \sum_{s} CSA_s^{f^a} y_s^{f^{a-pe}} \tag{10}$$

Case B:

$$\max \sum_{e^a} \sum_{g} EG_g x_g^{e^{a-pe}} \tag{11}$$

$$\min \sum_{e^a} \sum_{g} CGA_g^{e^a} x_g^{e^{a-pe}} \tag{12}$$

Case C:

$$\max \sum_{f^a} \sum_{s} \sum_{e^a} \sum_{g} (EG_g + ES_s) xy_{sg}^{ef^{a-pe}} \tag{13}$$

$$\min \sum_{f^a} \sum_{s} \sum_{e^a} \sum_{g} (CGA_g^{e^a} + CSA_s^{f^a}) xy_{sg}^{ef^{a-pe}} \tag{14}$$

In Case A, invaders attack only other substations, whereas in Case B, invaders attack power plants to interrupt other loads. Case C invaders could simultaneously attack other substations and power plants. In each case, the most effective substations or power plants with the lowest costs were determined. Each step and case has similar constraints. For example, the constraints for Case C in Step 2 are as follows:

$$P_g^{min} < Pgxy_g^{'ef^{a-pe}} < P_g^{max} \tag{15}$$

$$Q_g^{min} < Q_g xy_g^{'ef^{a-pe}} < Q_g^{max} \tag{16}$$

$$0 < S_l xy_s^{'ef^{a-pe}} < S_l^{max} \tag{17}$$

$$P_g^s xy_g^{'ef^{a-pe}} + \sum_{l} P_l^s xy_{s'}^{'ef^{a-pe}} = P_d^s xy_s^{'ef^{a-pe}} \tag{18}$$

$$Q_g^s xy_g^{'ef^{a-pe}} + \sum_{l} Q_l^s xy_{s'}^{'ef^{a-pe}} = Q_d^s xy_s^{'ef^{a-pe}} \tag{19}$$

$$S_s\left(V_s\right) = \left[V_s\right] Y_{bus}^{*} V_s^{*} \tag{20}$$

$$\begin{aligned}&(\sum\nolimits_{e^a} \sum_{g} \sum_{h}^{a} \sum_{k} (CCL_k^{h^a} + CVD_k^{e_g^a}) xz_{kg}^{eh^{a-pe}}\\ &\quad + \sum_{f^a} \sum_{s} \sum_{e^a} \sum_{g} (CGA_g^{e^a} + CSA_s^{f^a}) xy_{sg}^{ef^{a-pe}}) < AB\end{aligned} \tag{21}$$

$$\begin{aligned}&\sum\nolimits_{e^a} \sum_{g} \sum_{h}^{a} \sum_{k} (CCL_k^{h^a} + CVD_k^{e_g^a}) xz_{kg}^{'eh^{a-pe}}\\ &\quad > AB - \sum\nolimits_{e^a} \sum_{g} \sum_{h}^{a} \sum_{k} (CCL_k^{h^a} + CVD_k^{e_g^a}) xz_{kg}^{eh^{a-pe}}\end{aligned} \tag{22}$$

In this formulation, the active/reactive power output limitations of the power plants are defined in Eqs.(15) and (16). The constraint for the apparent power flow in power lines is given by (17). Equations (18) and (19) describe the active powerflow balance at each node. In this study, power flow problems were solved using MATPOWER, as defined in (20) [29]. The total cost in steps 1 and 2 must be less than the total attackers' budget defined in (21), and the reminder budget after step 1 must be less than the attack cost for attacks on other critical loads, as determined in (22).

According to the summary of the results of the first and second steps, substations and power plants determined in Step 1 are the first priority of enemies, and the reminder budget component in Step 2 is attacked as follows:

Case A:

$$VOS = [z_k^{h^{a-pe}}, y_s^{f^{a-pe}}] \tag{23}$$

Case B:

$$VOP = [x_{kg}^{e^{a-pe}}, x_g^{e^{a-pe}}] \tag{24}$$

Case C:

$$VOSP = [xz_{kg}^{eh^{a-pe}}, xy_{sg}^{ef^{a-pe}}] \tag{25}$$

Consequently, in each case, the priority of attackers, considering their resources and capabilities, is determined, which is, in fact, the value of substations and power plants. Therefore, VOS in (15) is the value of substations in Case A, VOP in (16) is the value of power plants in Case B, and VOSP in (17) is the value of substations and power plants simultaneously in Case C. Indeed, the arrangement of the elements of these vectors determines the priority of defense and attack. For example, the substation corresponding to the first {1} in vector VOS has the first priority for defense or attack. The algorithmic constraints of the proposed model correspond to the budget of the attackers. However, this method is performed by load priority, and as a result, this model can be implemented for small- or large-scale systems.

B. PLANNING FORMULATION

At this level, it is assumed that enemies will attack in accordance with the predictions in the pre-evaluation stage. The variables in the pre-evaluation stage are the specified parameters in the planning mode. The number and electrical position of newly constructed substations and power plants are variables at this level. The planning formulation in accordance with the planning model described in Section II is as follows.

Case A:

$$min \sum\nolimits_{ns} \sum\nolimits_{s} LO_s^{ns} VOS \tag{26}$$

$$min \sum\nolimits_{ns} \sum\nolimits_{s} CCS_s^{ns} VOS \tag{27}$$

Case B:

$$min \sum\nolimits_{mg} \sum_{g} \sum_{s} VD_s^{g-mg} VOP \tag{28}$$

$$min \sum\nolimits_{mg} \sum\nolimits_{g} \sum\nolimits_{s} CCP_s^{g-mg} VOP \tag{29}$$

Case C:

$$max \sum\nolimits_{mg} \sum_{g} \sum_{ns} \sum_{s} (LO_s^{ns} + VD_s^{g-mg}) VOSP \tag{30}$$

$$min \sum\nolimits_{mg} \sum_{g} \sum_{ns} \sum_{s} (CCS_s^{ns} + CCP_s^{g-mg}) VOSP \tag{31}$$

At the planning level, defenders want to minimize cut-off loads by priority by constructing new substations, power plants, or both to supply the attacked components in parallel. In case A, the enemies only attack substations with critical loads, case B only attacks power plants, and case C simultaneously attacks substations and power plants. In Case A, a multi objective optimization problem was solved using (26) and (27). In (26), the minimum load outage considering the pre-evaluation prediction level is solved, whereas in (27), the minimum construction cost for ns new substations that are constructed to supply loads in substation s in parallel is considered. In case B, a multi objective optimization problem is solved in (28) and (29). In (28), the minimum loads with a voltage drop of less than 0.95 p.u. were solved, while in (29), the minimum construction cost of a new power plant was determined. In case C, a multi objective optimization problem is solved in (30) and (31) that enemies simultaneously attack substations with loads and power plants; therefore, planners construct new substations and power plants simultaneously. *ns* and *mg* are the numbers of new substations and power plants, respectively. Considering budget restrictions, as mentioned in the pre-evaluation level, arranging the elements of vectors VOS, VOP, and VOSP determines the defense priority. The final solution (NS) is an arrow containing the number and location of newly constructed power plants and substations in parallel with existing power plants and substations, as follows:

$$NS = \overrightarrow{ij} \quad \mathrm{i} = 1, 2, \ldots, \mathrm{ns\ and\ j} = \{0, 1\} \tag{32}$$

$$NG = \overrightarrow{ij} \quad \mathrm{i} = 1, 2, \ldots, \mathrm{ng\ and\ j} = \{0, 1\} \tag{33}$$

$$NGS = \overrightarrow{ij} \quad \mathrm{i} = 1, 2, \ldots, \mathrm{ns\ or\ ng\ and\ j} = \{0, 1\} \tag{34}$$

j is a binary variable indicating whether planning is performed in relation to substation s or power plant g in the planning stage (1) or not (0). It is necessary for the next stages to show defended power plants and substations with an arrow, as shown below in Step 1.

$$CS = \begin{cases} 1 & if\ NS \neq 0 \\ 0 & if\ NS = 0 \end{cases} \quad \text{and } CS' \text{ is the inverse of CS} \tag{35}$$

Similarly, for steps 2 and 3, CG and CGS, respectively, and *CG′* and *CGS′* are their inverses.

Each case has similar constraints. For example, in Case C, the constraints are as follows:

Step 1:

Case A:

$$P_g^{min} < Pg < P_g^{max} \tag{36}$$

$$Q_g^{min} < Q_g < Q_g^{max} \tag{37}$$

$$0 < S_l < S_l^{max} \tag{38}$$

$$P_g^s + \sum_l P_l^s = P_d^s \tag{39}$$

$$Q_g^s + \sum_l Q_l^s = Q_d^s \tag{40}$$

$$S_s(V_s) = [V_s] Y_{bus}^* V_s^* \tag{41}$$

$$\sum\nolimits_{mg} \sum_{g} \sum_{ns} \sum_{s} (CCS_s^{ns} + CCP_s^{g-mg}) VOSP < PB \tag{42}$$

$$\begin{aligned} PB - \sum\nolimits_{mg} \sum_{g} \sum_{ns} \sum_{s} (CCS_s^{ns} + CCP_s^{g-mg}) VOSP \\ < \sum\nolimits_{mg} \sum_{g} \sum_{ns} \sum_{s} (CCS_s^{ns} + CCP_s^{g-mg}) VOSP\,(i+1) \end{aligned} \tag{43}$$

Constraints (36)–(41) are similar to constraints (15)–(20) in the pre-evaluation stage in the general case. Constraint (42) shows that the construction cost must be less than the planning budget, and constraint (43) describes that the arranging element of the VOSP determines the priority corresponding substations and power plants for defense.

C. HARDENING FORMULATION

Hardening formulation according to its model in previous section is as follows.

Case A:

$$max \sum\nolimits_{h^h, f^h} \sum\nolimits_{k,s} HL_{k,s}^{h^h, f^h} \times VOS \times CS' \times z_{k,s}^{h^h, f^h} \tag{44}$$

$$min \sum_{h^h, f^h} \sum_{k,s} HC_{k,s}^{h^h, f^h} \times VOS \times CS' \times z_{k,s}^{h^h, f^h} \tag{45}$$

Case B:

$$max \sum\nolimits_{e^h} \sum\nolimits_{g} \sum\nolimits_{k,s} VD_{k,s}^{e^h-g} \times VOP \times CG' \times x_g^{e^h} \tag{46}$$

$$min \sum\nolimits_{e^h} \sum\nolimits_{g} \sum\nolimits_{k,s} HC_{k,s}^{e^h-g} \times VOP \times CG' \times x_g^{e^h} \tag{47}$$

Case C:

$$\begin{aligned} max \sum\nolimits_{e^h} \sum\nolimits_{g} \sum\nolimits_{h^h f^h} \sum\nolimits_{k,s} (HL_{k,s}^{h^h f^h} + VD_{k,s}^{e^h-g}) \\ \times VOSP \times CGS' \times xz_{g,k,s}^{e^h, h^h f^h} \end{aligned} \tag{48}$$

$$\begin{aligned} min \sum\nolimits_{e^h} \sum\nolimits_{g} \sum\nolimits_{h^h f^h} \sum\nolimits_{k,s} (HC_{k,s}^{h^h f^h} + HC_{k,s}^{e^h-g}) \\ \times VOSP \times CGS' \times xz_{g,k,s}^{e^h, h^h f^h} \end{aligned} \tag{49}$$

Steps 1 and 2 are combined, which means that the critical load has hardened in the first priority and other loads in the second priority, with values determined in the pre-evaluation stage. The priority of power plants and substations for hardening is determined in accordance with their values, that is, VOS, VOP, and VOSP. The use of CS', CG' and CGS' defends elements in the planning mode to eliminate the hardening stage. Each case has similar constraints. For example, in Case C, the constraints are as follows:

Step 1:

Case A:

$$P_g^{min} < Pg < P_g^{max} \tag{50}$$

$$Q_g^{min} < Q_g < Q_g^{max} \tag{51}$$

$$0 < S_l < S_l^{max} \tag{52}$$

$$P_g^s + \sum_{l} P_l^s = P_d^s \tag{53}$$

$$Q_g^s + \sum_{l} Q_l^s = Q_d^s \tag{54}$$

$$S_s\,(V_s) = [V_s]\, Y_{bus}^* V_s^* \tag{55}$$

$$\begin{aligned} \sum\nolimits_{e^h} \sum_{g} \sum_{h^h, f^h} \sum_{k,s} (HC_{k,s}^{h^h, f^h} + HC_{k,s}^{e^h-g}) \times VOSP \\ \times CGS' < HB \end{aligned} \tag{56}$$

$$\begin{aligned} HB - \sum\nolimits_{e^h} \sum_{g} \sum_{h^h, f^h} \sum_{k,s} (HC_{k,s}^{h^h, f^h} + HC_{k,s}^{e^h-g}) \\ \times CGS' \times VOSP\,(1, 2, \ldots, i) \\ < \sum\nolimits_{e^h} \sum_{g} \sum_{h^h, f^h} \sum_{k,s} (HC_{k,s}^{h^h, f^h} + HC_{k,s}^{e^h-g}) \\ \times CGS' \times VOSP(i+1, i+2, \ldots, end) \end{aligned} \tag{57}$$

Constraint (56) states that the hardening cost must be less than the hardening budget, and constraint (57) shows that the arranging element of the VOSP determines the priority corresponding to substations and power plants for hardening.

D. ATTACK FORMULATION

Attack formulation in accordance with its model is as follows.

Case A:

$$max \sum\nolimits_{h^a, f^a} \sum\nolimits_{k,s} AL_{k,s}^{h^a, f^a} \times VOS \times z_{k,s}^{\prime h^h, f^h} \times z_{k,s}^{h^a, f^a} \tag{58}$$

$$min \sum\nolimits_{h^a, f^a} \sum\nolimits_{k,s} AC_{k,s}^{h^a, f^a} \times VOS \times z_{k,s}^{\prime h^h, f^h} \times z_{k,s}^{h^a, f^a} \tag{59}$$

Case B:

$$max \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{k,s} VD_{k,s}^{e^a-g} \times VOP \times x'^{e^h}_{g} \times x_g^{e^a} \tag{60}$$

$$min \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{k,s} AC_{k,s}^{e^a-g} \times VOP \times x_g^{\prime e^h} \times x_g^{e^a} \tag{61}$$

Case C:

$$\begin{aligned} m\ max \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{h^a, f^a} \sum\nolimits_{k,s} (AL_{k,s}^{h^a, f^a} + VD_{k,s}^{e^a-g}) \\ \times VOSP \times xz'^{e^h, h^h, f^h}_{g,k,s} \times xz_{g,k,s}^{e^a, h^a, f^a} \end{aligned} \tag{62}$$

$$\begin{aligned} min \sum\nolimits_{e^a} \sum\nolimits_{g} \sum\nolimits_{h^a, f^a} \sum\nolimits_{k,s} (AC_{k,s}^{h^a, f^a} + AC_{k,s}^{e^a-g}) \\ \times VOSP \times xz'^{e^h, h^h, f^h}_{g,k,s} \times xz_{g,k,s}^{e^a, h^a, f^a} \end{aligned} \tag{63}$$

In the above formulation, Steps 1 and 2 are combined, which means that it is attacked by the critical load in the first priority and other loads in the second priority with values determined in the pre-evaluation stage. In this stage VOS, VOP, VOSP, $z_{k,s}^{\prime h^h, f^h}$, $x'^{e^h}_{g}$ and $xz'^{e^h, h^h, f^h}_{g,k,s}$ are constant value and $z_{k,s}^{h^a, f^a}$, $x_g^{e^a}$ and $xz_{g,k,s}^{e^a, h^a, f^a}$ are variables. The priority of power plants and substations for attack is determined according to their values, that is, VOS, VOP, and VOSP. With using of $z_{k,s}^{\prime h^h, f^h}$, $x'^{e^h}_{g}$ and $xz'^{e^h, h^h, f^h}_{g,k,s}$ that is inverse of $z_{k,s}^{h^h, f^h}$, $x_g^{e^h}$ and $xz_{g,k,s}^{e^h, h^h, f^h}$ and determined in hardening stage, defended elements in hardening mode eliminate for attack stage and conditions in table 1 to be applied in constraints. Each case has similar constraints. For example, in Case C, the constraints are as follows:

$$P_g^{min} < Pg \times xz_{g,0,0}^{\prime e^a,0,0} < P_g^{max} \tag{64}$$

$$Q_g^{min} < Q_g \times xz_{g,0,0}^{\prime e^a,0,0} < Q_g^{max} \tag{65}$$

$$0 < S_l < S_l^{max} \tag{66}$$

$$(P_g^s \times xz_{g,0,0}^{\prime e^a,0,0}) + \sum_l P_l^s = (P_d^s \times xz_{0,k,s}^{\prime 0,,h^a,f^a}) \tag{67}$$

$$S_s\,(V_s) = [V_s]\,Y_{bus}^* V_s^* \tag{68}$$

$$\sum\nolimits_{e^a} \sum_g \sum_{h^a,f^a} \sum_{k,s} (AL_{k,s}^{h^a,f^a} + VD_{k,s}^{e^a-g}) \times VOSP \times xz'^{e^h,h^h,f^h}_{g,k,s} < AB \tag{69}$$

$$\sum\nolimits_{e^a} \sum_g \sum_{h^a,f^a} \sum_{k,s} (AL_{k,s}^{h^a,f^a} + VD_{k,s}^{e^a-g}) \times VOSP \times xz'^{e^h,h^h,f^h}_{g,k,s} < AB \tag{70}$$

$$\begin{aligned} AB - \sum\nolimits_{e^a} \sum_g \sum_{h^a,f^a} \sum_{k,s} (AL_{k,s}^{h^a,f^a} + VD_{k,s}^{e^a-g}) \\ \times xz'^{e^h,h^h,f^h}_{g,k,s} \times VOSP\,(1, 2, \ldots, i) \\ < \sum\nolimits_{e^a} \sum_g \sum_{h^a,f^a} \sum_{k,s} (AL_{k,s}^{h^a,f^a} + VD_{k,s}^{e^a-g}) \\ \times xz'^{e^h,h^h,f^h}_{g,k,s} \times VOSP(i{+}1, i{+}2, \ldots, end) \end{aligned} \tag{71}$$

$xz_{g,0,0}^{\prime e^a,0,0}$ is a vector equal to $xz_{g,k,s}^{e^a,h^a,f^a}$ but not attacked power plants are {1}; therefore, power plant constraints are applied only to power plants that are not attacked. As the same way, $xz_{g,0,0}^{\prime e^a,0,0}$ is a vector equal to $xz_{g,k,s}^{e^a,h^a,f^a}$ but only not attacked substations are {1} and therefore substation constraints are applied only to not attacked substation. Constraint (70) states that the attack cost must be less than the attack budget, and constraint (71) shows that the arranging element of VOSP determines the priority corresponding to substations and power plants for attack. The algorithm in table 1 is a constraint attack method based on the defense method, which is added to other constraints. In the proposed model, the priority value of each element is used for hardening and attack formulation. Therefore, this formulation can be used in any system regardless of its scale.

E. RECOVERY FORMULATION

The recovery stage was performed after the occurrence of an attack. It is assumed that the recovery steps consist of (Automatic Voltage Regulator). of the power plants at the first level, and load shedding in the next step. A recovery flowchart is shown in Fig. 2.

F. COST OF HARDENING FORMULA

It is assumed that there is a strategy for hardening, as mentioned in the hardening model. Therefore, three hardening costs exist related to each strategy, as follows:

G. HUMAN PROTECTION COST FOR SUBSTATIONS (HPCS) AND POWER PLANTS (HPCG)

Human protection (HP) is hardened by a human guard, and its cost for one year is determined by the following formulation:

$$HPCS = (CGPS \times CPDS \times 8760 + CADS) \times HPSC \tag{72}$$

$$HPCG = (CGPG \times CPDG \times 8760 + CADG) \times HPGC \tag{73}$$

In (72), *HPCS*, *CGPS*, *CPDS* and *CADS* are the cost of hardening by human protection ($/Year), cost of guard for human protection to a substation ($/hour), cost of the number of people to defend against a substation, and the cost of ammunition for defense to a substation ($/year), respectively. The corresponding formula for power plants is given by Equation (73): Each substation and power plant has a special characteristic that results in different protection costs. This difference is affected by a coefficient called the human-protected substation coefficient and the power plant coefficient, which are shown by *HPSC* and *HPGC*. The HPCS and HPCG for 30 years are shown by HPCS30 and HPCG30, respectively, calculated as follows:

$$HPCS30 = HPCS \times 30 \tag{74}$$

$$HPCG30 = HPCG \times 30 \tag{75}$$

H. PHYSICAL PROTECTION COST FOR SUBSTATIONS (PPCS) AND POWER PLANTS (PPCG)

Physical protection (PP) is hardened by physical actions and its cost for one year, as determined by the following formulation:

$$PPCS = PCS \times PSC \tag{76}$$

$$PPCG = PCG \times PGC \tag{77}$$

In (76), *PPCS* and *PCS* are the cost of hardening by physical protection ($/Year) and the sum of cost of different strategy accomplished for physical protection ($), respectively. The corresponding formula for power plants is given in (77). Each substation and power plant has a special characteristic that results in different protection costs. This difference is affected by the substation coefficient and power plant coefficient for physical protection, as shown by *PSC* and *PGC*. The PPCS and PPCG for 30 years are shown by PPCS30 and PPCG30, respectively, calculated as follows:

$$PPCS30 = PPCS + (29 \times \frac{PPCS}{3}) \tag{78}$$

$$PPCG30 = PPCG + (29 \times \frac{PPCG}{3}) \tag{79}$$

In (78) and (79), it is assumed that the total cost is spent in the first year, and in the other years, only $\frac{1}{3}$ costs are spent on the restoration of the previous structure.

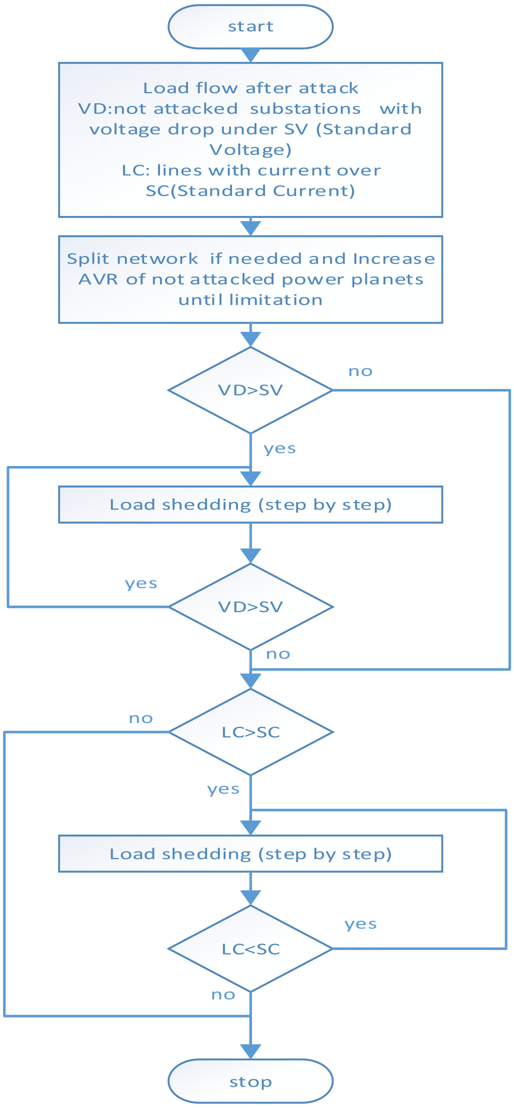
start
Load flow after attack
VD:not attacked substations with voltage drop under SV (Standard Voltage)
LC: lines with current over SC(Standard Current)
Split network if needed and Increase AVR of not attacked power planets until limitation
VD>SV
no
yes
Load shedding (step by step)
yes
VD>SV
no
no
LC>SC
yes
Load shedding (step by step)
yes
LC<SC
no
stop

FIGURE 2. Flowchart of recovery stage.

I. TOTAL PROTECTION COST FOR SUBSTATIONS (TPCS) AND POWER PLANTS (TPCG)

If defenders use human protection and physical protection together, this is called total protection, and its cost is calculated as the sum of the human and physical protection costs.

J. COST OF ATTACK FORMULA

It is assumed that there is an attack strategy, as mentioned in the previous section; thus, three attack costs exist related to each strategy, as follows.

K. ATTACK COST TO UNPROTECTED SUBSTATIONS (ACUS) AND POWER PLANTS (ACUG)

$$ACUS = ACS \times ASC \tag{80}$$

$$ACUG = ACG \times AGC \tag{81}$$

In (80), *ACUS* and *ACS* are the attack cost to unprotected substations ($) and the sum of cost for attack to a substation included human and ammunition cost ($), respectively. The corresponding formula for power plants is given by (81). Each substation and power plant has special characteristics that result in different attack costs. It is affected by a coefficient that named unprotected substation coefficients and unprotected power plant coefficients for attack, as shown by *ASC* and *AGC*.

L. ATTACK COST TO HUMAN PROTECTED SUBSTATIONS (HACS) AND POWER PLANTS (HACG)

The attack cost on a substation or power plant that is protected by human protection is determined by the following formulation:

$$HACS = (CGAHS \times CPAHS \times 8760 + CAAHS) \times AHSC \tag{82}$$

$$HACG = (CGAHG \times CPAHG \times 8760 + CAAHG) \times AHGC \tag{83}$$

In (82), *HACS*, *CGAHS*, *CPAHS* and *CAAHS* are the cost of attack on a human-protected substation ($), cost of guard for attack to human protected substation ($/Hour), cost of the number of people to attack a human-protected substation, and the cost of ammunition for an attack on a human-protected substation ($), respectively. The corresponding formula for power plants is given in (83). Each substation and power plant has special characteristics that result in different attack costs. This difference is affected by a coefficient called the attack on the human-protected substation coefficient and the power plant coefficient, which is shown by *AHSC* and *AHGC*.

M. ATTACK COST TO PHYSICAL PROTECTED FOR SUBSTATIONS (PACS) AND POWER PLANTS (PPCG)

The attack cost on a substation or power plant that is protected by physical protection is determined by the following formulation:

$$PACS = (CGAPS \times CPAPS \times 8760 + CAAPS) \times APSC \tag{84}$$

$$PACG = (CGAPG \times CPAPG \times 8760 + CAAPG) \times APGC \tag{85}$$

In (84), *PACS*, *CGAPS*, *CPAPS* and *CAAPS* are the cost of attacking a physically protected substation ($), cost of guard for attack to physical protected substation ($/Hour), cost of the number of persons to attack a physically protected substation, and the cost of ammunition for attacking a physically protected substation ($), respectively. The corresponding formula for power plants is given in (85). Each substation and power plant has special characteristics that result in different attack costs. This difference is affected by a coefficient called the attack on the physically protected substation coefficient and power plant coefficient, which is shown by *APSC* and *APGC*.

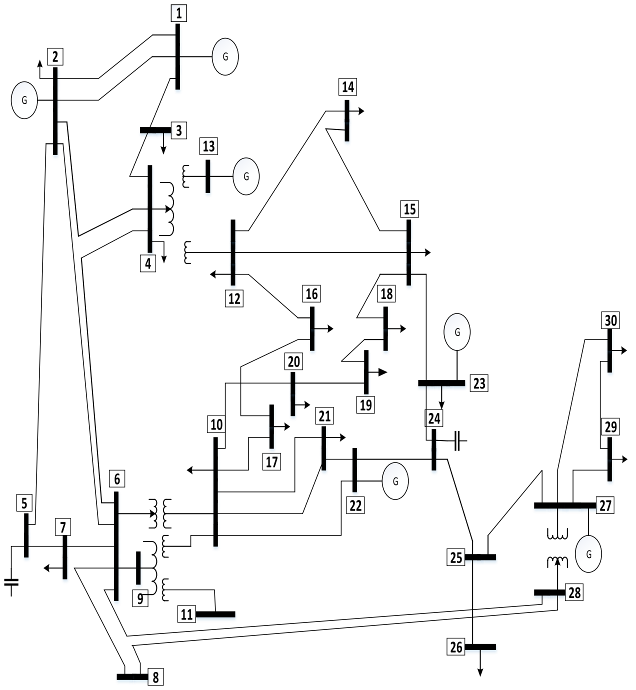

FIGURE 3. Single line diagram - IEEE-30 bus test system.

N. TOTAL ATTACK COST FOR SUBSTATIONS (TACS) AND POWER PLANTS (TACG)

In the case where attackers attack a human and a physically protected substation or power plant together, in the first assumption, it is called a total attack, and its cost is calculated by the sum of attacks on human and physical protected costs. In the second assumption, attackers are unable to attack the substation or the power plant. In this study, the second assumption was made.

O. LOAD FLOW FORMULATION

In this study, the MATPOWER package was used to implement and run load flow in necessary steps, such as pre-evaluation, planning, and attack, and to investigate the influence of each countermeasure on recovery [35]. The power flow formulation of MATPOWER completely covers the requirements of all steps.

IV. CASE STUDY

This case study uses the IEEE-30 bus test system. The one-line diagram is shown in Fig. 3, and the system data were taken from references [34], [36], [37], [38], [39], [40], [41]. It is worth mentioning that the proposed method can be applied to larger power systems, as the value of elements and load priority can be considered for all electrical components, regardless of the power system scale. Moreover, the new four-level proposed method requires less computational effort, as the main problem is divided into four simpler optimization problems with less computational complexity.

The DG locations are different in various references, and this study uses [30] for these locations, as shown in Fig. 2.

A. BASIC DATA

Basic data assumed in this paper or obtained from formula is as follows.

1) BASIC CRITICAL LOAD DATA

In this text critical load is assumed as shown in Table 2.

TABLE 2. Critical load and bus.

Number of bus	Critical load (MW)
7	12
16	2
24	1
30	1.5

It is assumed that substation 7 is 230/132 KV and the others are 132/20 KV.

2) BASIC PLANNING DATA

The power network element costs are variable, but it is assumed that the average of the 230/132 KV substation construction cost is $ 11,700,000, $ and that of 132/20 KV is 6,700,000 $ [35]. In addition, the average construction cost of a 100 MVA substation is approximately 100,000,000 $.

3) BASIC HARDENING DATA

It is assumed that the budget of defenders is provisioned annually; however, for a better comparison between different strategies, the cost is 30 years, which is a useful life for substations and power plants. In this text, it is considered that the basic armed guard's cost for substations (CGPS) is $25 per hour for one person [36] and 10 persons need to protect each substations (CPDS). Also the cost of ammunition defenders for substation (CADS) is considered to be $50000 for a year. For power plants, it is assumed that 20 persons are required to protect each power plant (CPDG), and the remaining data are the same as for the substation. Based on these assumptions, the cost of hardening by human protection for substations (HPCS) and power plants (HPCG) ($/Year) after applying the human protected substation and power plant coefficient (HPSC) and (HPGC) are determined. For physical protection, it is assumed that the sum of cost of different strategy accomplished for physical protection for substations (PCS) is $3,000,000 and that for power plants (PCG) is $5,000,000. By this assumptions cost of hardening by physical protection for substations (PPCS) and power plants (PPCG) ($/year) after applying the physical substation and power plant coefficients (PSC) and (PGC) are determined. The PPCS and PPCG for 30 years were determined using Equations (78) and (79), respectively. The total protection cost is calculated as the sum of human and physical protection costs.

4) BASIC ATTACK DATA

For attack costs to unprotected substations (ACUS) and power plants (ACUG), it is assumed that the sum of the cost of attack to a substation, including human and ammunition costs (ACS), is $1,000,000 and for power plants is $4,000,000. After applying the unprotected substation and power plant coefficients for attack (ASC) and (AGC), the attack costs to the unprotected substations and power plants are determined. It is considered that enemies need experienced armed guard for attack with a cost of $100 per hour for one person for substations (CGAHS) [36] and 20 persons need to protect each substations (CAAHS). Also the cost of ammunition need for attack to substation (CAAHS) is considered to be $100,000. The corresponding data for the power plants (CGAHG), (CPAHG), and (CAAHG) were $150 per hour for one person, 50 person and $500,000, respectively. After applying an attack to a human-protected substation, the power plant coefficient (AHSC) and (AHGC). The attack costs for human-protected substations and power plants are determined. The corresponding data for attacks on physically protected substations (CGPAS), (CPAPS), and (CAAPS) were $100 per hour for one person, 25 person and $400,000, respectively, and for power plants (CGPAG), (CPAPG), and (CAAPG) were $150 per hour for one person, 55 person and $800,000, respectively. The attack costs for the physically protected substations and power plants were determined. In this study, it was assumed that enemies cannot attack humans, physically protected substations, or power plants.

5) BASIC RECOVERY DATA

The two steps were assumed to be in the recovery stage. The first step is to increase the AVR of the power plants, which can change the output power-plant voltage to ±2%. The second is load shedding, where each step is 0.3 per unit. It was assumed that the critical load voltage is 0.95 per unit and the critical line current was equal to the thermal capacity of each line.

B. RESULTS

The entire stage was performed in accordance with their model and the formula mentioned above, and the results are shown below.

1) CASE 1: ATTACK TO THE SUBSTATIONS

In the first case, it is assumed that power plants are completely protected by defenders and invaders are only able to attack substations.

a: SIMULATION WITHOUT PLANNING (DAD MODEL)

In this case, the classic three-layer method for resiliency that is three layer method was used. The results are as follows:

i) HARDENING RESULTS

The results are presented in Table 3. For hardening cost for 30 years, it is assumed that critical substations need to protect by HPPS method for 30 years without consideration inflation which invaders won't be able to attack to any substations. Recall that the budget after hardening is not sufficient to protect any other substations. Therefore, the critical loads on the 24 and 30 buses were exposed to attacks.

TABLE 3. Hardening results before planning (DAD model) for case1.

Total Hardening Budget	$11,000,000
Hardening substations and strategy	7(PPS)/16(PPS)
Hardening Cost (1 year)	$10,780,000
Hardening Cost (30 year)	$396,800,000

ii) ATTACK RESULTS

Results are shown in Table 4.

It is shown that after the hardening step, substations (30) and (16) are attacked and their critical loads are cut off. The remind budget is not sufficient to attack other critical loads; therefore, (8) and (12) noncritical load substations are in attack in accordance with their value and remind the budget. Recall that the budget after the second step is not sufficient to attack any other substations. The total number in table 4 is 1 year. If the defenders have used the HPP method for 30 years for substations with critical loads, attackers cannot attack these substations.

TABLE 4. Attack results before planning (DAD model).

Total Attack Budget	$5,000,000
Attack to critical load substations	30(HAS)/24(HAS)
Attack to conventional substations	8(HAS)/12(HAS)
Cut off critical loads (MW)	2.5
Cut off non-critical loads (MW)	58
Total Attack Cost	$5,000,000
Remind Attack Budget	$0

ii) RECOVERY RESULTS

Owing to the direct attack on substations, there is no out-of-range bus voltage or line current. Therefore, this was not a recovery step.

As a result, it is shown 19.3 MW loads of critical buses 30 and 24 cut off while 2.5 thereof is critical. The interruption cost of these curtailment loads with the assumption 6.29 $/KW for critical loads and 3.59 $/KW for other loads is $224,000 [37].

If defenders want to prevent cutting off the critical load in substations, it is necessary to protect buses7, 16, 30, and 24 in the HPP methods and need $23,132,000 ($/year) to protect them. Assuming that 30 years is a useful life for each substation, defenders need $396,800,000 and therefore they need $386,020,000 extra budget to prevention cutting off the entire critical load for 30 years.

b: SIMULATION FOR FOUR LAYER MODEL (DDAD MODEL)

In this stage, planning was added before hardening as the first step of defense. In this method, defenders construct several new simple substations near critical load substations to feed the loads in parallel. It is assumed that the new substations are simple at half the price because they need to feed only the critical loads. According to the pre-evaluation model simulation in the preceding section, it is suggested that five new simple substations be constructed near each critical load bus to avoid cutting off the critical loads. Therefore, in accordance with the construction price in the previous section and the above assumptions, defenders only need $79,500,000 and therefore need $68,500,000 extra budget for 30 years. As a result, the total cost of (DDAD) model was $317,520,000 less than (of) conventional DAD model for 30 years in this case. Then, all steps are performed, and the attack results change, as listed in Table 5.

As shown in Table 5, the attacker's strategy was changed. Enemies cannot attack critical loads, and only noncritical loads are in attack, with an interruption cost of $289,000.

TABLE 5. Attack results after planning (DDAD model).

Total Attack Budget	$5,000,000
Attack to critical load substations	-
Attack to conventional substations	8/ 12 / 2/ 21 (HAS)
Cut off critical loads (MW)	-
Cut off non-critical loads (MW)	80.4
Total Attack Cost	$4,400,000
Remind Attack Budget	$600,000

c: SIMULATION WITH UNCERTAIN ATTACKERS' BUDGET

If defenders do not know the invaders' budgets and resources, the problem is solved using probability methods. It is assumed that there is a low probability that an enemy's budget will be very low or very high. As a result, a normal distribution with a mean and variance $5,000,000 and $1,800,000, respectively, was considered for the invaders' budget. The problem was solved using the previous formula and the Monte Carlo method to select the best strategy for defense, and the results are shown in Fig. 4.

It is shown that defenders select strategy 1 because this strategy has the maximum number of cases (55%). The solution for (DDAD) model does not change in this manner.

2) CASE 2: ATTACK TO THE SUBSTATIONS AND POWER PLANTS SIMULTANEOUSLY

In the second case, it is assumed that the enemies will be able to simultaneously attack substations and power plants. Attacks on power plants cause a bus voltage drop or exceed limit lines or other power plants. The simultaneous attack of two or three power plants has destructive effects. These effects are shown in Appendix B. The outages of power plants (1,2), (3,4), (3,5), (4,5), and (3,4,5) cause blackouts.

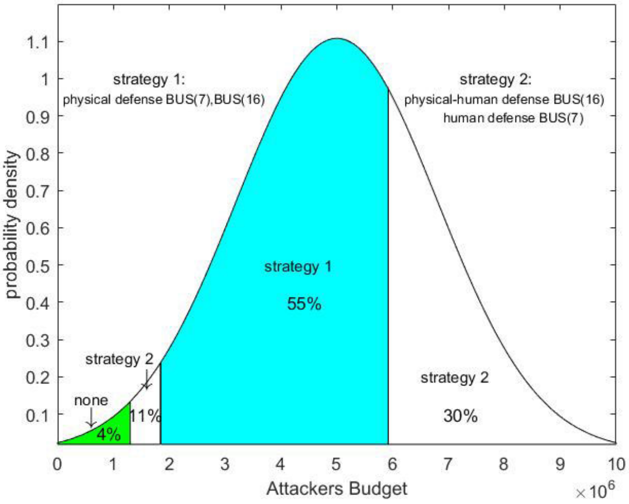

FIGURE 4. Simulation for uncertain attackers' budget with normal distribution.

TABLE 6. Hardening results before planning (DAD model) for case1.

Total Hardening Budget	$43,000,000
Hardening substations, power plants and strategy	GEN1,GEN2(HPPG) GEN3 (PPG) 16(HPPS)/30(HPS)
Hardening Cost (1 year)	$42,132,000
Hardening Cost (30 year)	$1,483,909,999

TABLE 7. Attack results before planning (DAD model).

Total Attack Budget	$11,600,000
Attack to critical load substations and power plants	GEN3(PAG) / GEN4(UAG)
Attack to conventional substations	14(UAS)
Cut off critical loads (MW)	16.5
Cut off non-critical loads (MW)	118.4
Total Attack Cost	$10,740,000
Remind Attack Budget	$860,000

a: SIMULATION WITHOUT PLANNING (DAD MODEL)

In this case, the conventional method for resiliency, that is, the three-layer method (DAD), was used. The results are as follows:

i) HARDENING RESULTS

The results are presented in Table 6. For a hardening cost of 30 years, it is assumed that the critical substations and total power plants must be protected by the HPPS.

and the HPPG method for 30 years without considering inflation, which means that invaders will not be able to attack substations or power plants. Recall that the budget after hardening is not sufficient to protect any other substations or power plants. Therefore, the critical loads in buses 7, 24, and 30 and power plants 3 to 6 were exposed to the attack.

ii) ATTACK RESULTS

Results are shown in table (7).

After the hardening step, (GEN3) and (GEN4) power plants are attacked, which causes the power network to blackout. The remind budget is not sufficient to attack other critical loads; therefore, (14) noncritical load substations are in attack in accordance with their value and remind the budget. Recall that the budget after the second step is not sufficient to attack any other substations. The total number in table 4 is 1 year. If defenders have used the HPP method for 30 years in substations with critical loads and power plants, attackers cannot attack these elements.

iii) RECOVERY RESULTS

Because of the overlimit gen (2) and voltage drop, most of the buses in this case cannot save the entire network by using AVR and load shedding. Therefore, defenders must split the network to survive in some parts of the system as the first step toward recovery. By creating an island with genes (5) and (6) and buses 12, 14, 15, 16, 17, 18, 19, 20, and 24, it is possible to save this part of the network. In the second step of recovery, the AVR of generators (5) and (6) is increased such that its voltage increase to 1.02 p.u.. In the third step, the load shedding and loads of bus 17,19 and 20 decrease by 30%, and the loads of buses 12 and 14 decrease by 20%..After three steps, the load shedding of all the voltages of the buses and other limits was within the standard range.

As a result, it is shown that only after recovery, 3 MW loads of critical buses 16, 24 and 49.11 of other loads will be saved. As a result 13.5 MW of critical loads and 123.59 MW of conventional loads are cut off, with an interruption cost of $528,900.

If defenders want to prevent cut-off critical load in substations, it is necessary to protect buses7, 16, 30, 24, and total power plants using HPP methods and require a total $1,483,909,999 and $1,440,910,000 extra budget to prevent cut-off whole critical loads for 30 years.

b: SIMULATION FOR FOUR LAYER MODEL (DDAD MODEL)

According to the pre-evaluation model simulation, three new simple substations near each critical load bus and three new power plants parallel to power plants (3) or (4) were constructed. As a result, defenders only need $474,700,000 and therefore need $463,100,000 extra budget for 30 years. As a result, the total cost of (DDAD) model was $977,810,000 less than (of) conventional DAD model for 30 years in this case. Then, all steps are performed, and the attack results change, as listed in Table 8.

As shown in Table 8, the attacker's strategy was changed. Enemies cannot attack critical loads, and only noncritical loads are in attack, with an interruption cost of $ 462,751.

c: SIMULATION WITH UNCERTAIN ATTACKERS' BUDGET

In the previous section, a normal distribution with a mean and variance $5,000,000 and $1,800,000, respectively, was considered for the invaders' budget. As shown in Fig. 5, the best strategy for defense is Strategy 1, which is selected by 60.7% of defenders.

TABLE 8. Attack results after planning (DDAD model).

Total Attack Budget	$11,600,000
Attack to critical load substations	-
Attack to conventional substations	8 / 12 /2 / 21/4/17/19/10/14/15/20 (HAS)
Cut off critical loads (MW)	-
Cut off non-critical loads (MW)	128.9
Total Attack Cost	$10,800,000
Remind Attack Budget	$800,000

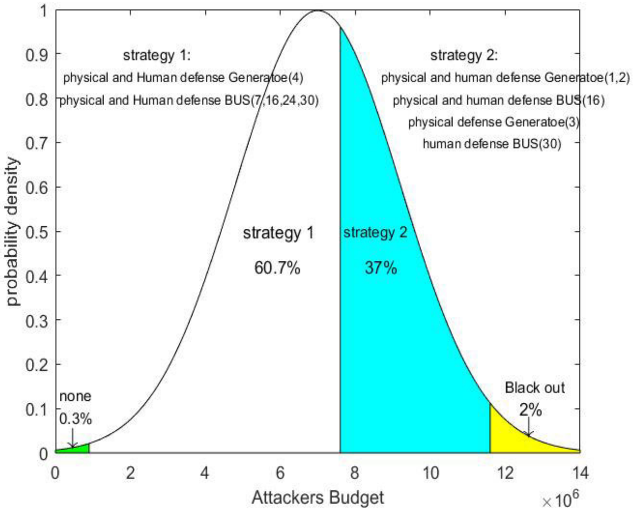

FIGURE 5. simulation for uncertain attackers' budget with normal distribution.

TABLE 9. Summarized the result of case 1 and case 2.

	(DAD) Model Critical load cut off (MW)	(DDAD) Model Critical load cut off (MW)	Saving budget (DDAD) model on (DAD) model ($)
Case 1	2.5	-	317,520,000
Case 2	13.5	-	977,810,000

C. SUMMARY OF THE RESULTS

Just to summarize the results, table 9 compromise pervious cases.

As shown in the new (DDAD) model, no critical load is cut off with a very small defense budget for protecting critical loads for over 30 years. As shown in Table 9, in the new (DDAD) model in case 1, $317,520,000 and in case 2 $977,810,000 are saved compared with the classic (DAD) model. It is also clear by comparing Tables 6 and 7 that with the same budget, the attackers in the proposed (DDAD) model can have fewer hits than those in the classic (DAD) model, while the defenders need less budget. On the other hand, defenders must protect substations and power plants in (DAD) model for 30 years, which causes hardship and exhaustion of defenders. In addition, outfit guard groups for 30 years have difficulty with ancillary expenses, which is another disadvantage of the classic (DAD) model. In addition, in (DDAD) model, some substations and power plants are added to the network, and network assets are increased, while the entire budget in (DAD) model is 30 years.

V. CONCLUSION

In this study, a new strategy is proposed to improve power system resilience against human attacks by adding a new defensive level to the classic solution. The priorities of the loads, power plants, and substations were considered. The strategy includes a four-level resilience enhancement model, DDAD, which was proposed for intelligent human attacks. The results show that adding a new planning level to conventional DAD results in a more effective method requiring a lower resilience enhancement budget in comparison to the classical DAD method.

Looking at the proposed model more closely, new power plants and substations were added to the network to increase the resilience of the power system by selecting the most sensitive components. In Case 1, defenders can save \$317,520,000 in their budget assigned to support critical loads. In case 2, with simultaneous attacks on substations and power plants, \$979,810,000 of was saved. Adding the new planning layer leads to an increase in the power system components in a 30-year period compared to conventional DAD, which requires 30-year physical guarding. In other words, in the new method, the budget is used to construct the electrical infrastructure, whereas in the classical model, the budget is spent on physical protection. In this study, the defender and attacker had independent strategies regarding budget limitations. In future studies, we will simultaneously consider all power network sections, including power plants, substations, and transmission lines. Moreover, the ever-increasing penetration of renewable energy systems and their effects on power system resilience are interesting topics for future studies.

NOMENCLATURE

A. STETS AND INDICES

$h^h \in H^H$	Hardening strategies for substations with critical loads
$h^a \in H^A$	Attack strategies for substations with critical loads
$e^h \in E^H$	Hardening strategies for power plants
$e^a \in E^A$	Attack strategies for power plants
$f^h \in F^H$	Hardening strategies for substations
$f^a \in F^A$	Attack strategies for substations
$k \in K$	Substations with critical loads
$s \in S$	Substations

$g \in G$	Generators
$l \in L$	Power lines
ns	Number of new substations constructed to supply loads in parallel with old substations
mg	Number of new power plants constructed to supply loads in parallel with the old power plant g

B. PARAMETERS

ES_s	Effectiveness criterion for substations
EG_g	Effectiveness criterion for power planets
$IC1$	Interruption cost for different loads for 1houer
P_d^s/Q_d^s	Active / Reactive power load demand in substation s
P_g^{min}/P_g^{max}	Active power output range of power plants
Q_g^{min}/Q_g^{max}	Reactive power output range of power plants
S_l^{max}	Maximum apparent power flow in line l
$CCL_k^{h^a}$	Cost of attack to substation k with strategy h^a(\$)
$CVD_k^{e^{a-g}}$	Cost of attack to power plant g with strategy e^a that caused to voltage drop less than 0.95 p.u. in substation k (\$)
$CGA_g^{e^a}$	Cost of attack to power plant g with strategy e^a(\$)
$CSA_s^{f^a}$	Cost of attack to substation s with strategy f^a(\$)
Y_{bus}	Y bus of network
AB	Attack Budget
CCS_s^{ns}	Construction cost for ns^{th} new substation due to supply loads in substation s in parallel
CCP_s^{g-mg}	Construction cost for mg^{th} new power plant mgth due to supply in parallel with power plant g to increase the voltage of substation s to over 0.95 p.u.
PB	Planning Budget
$HC_{k,s}^{h^h,f^h}$	Hardening costs to substations k and s with strategies h^h and f^h respectively (\$)
$HC_{k,s}^{e^h-g}$	Hardening Cost for power plant g to increase voltage of substation k and s over 0.95 p.u. respectively, to prevent attacks after hardening with strategy e^h (\$)
HB	Hardening Budget
$AC_{k,s}^{h^a,f^a}$	attack cost to substations k and s with strategies h^a and f^a respectively (\$)
$AC_{k,s}^{e^a-g}$	Attack cost for power plant g to decrease voltage of substation k and s under 0.95 p.u. respectively, owing to attack with strategy e^a (\$).

C. VARIABLES

The $z_k^{h^a-pe}$	binary variables indicate whether the h^ath attack strategy to substation k in the pre-evaluation stage selected (1) or not (0).
$x_g^{e^h}$	Binary variables indicate whether e^hth hardening strategy at generator g is selected (1) or not (0).
$x_{kg}^{e^a-pe}$	binary variables indicate whether an e^ath attack strategy to power plant g causes a voltage to critical loads substation k less than 0.95 in the pre-evaluation stage selected (1) or not (0).

$xz_{kg}^{eh^{a}-pe}$ Binary variables indicate whether the h^ath attack strategy to substation k and the e^ath attack strategy to power plant g simultaneously cause a load outage or voltage drop of less than 0.95 to the critical load substation k in the pre-evaluation stage selected (1) or not (0).

$x_g^{e^{a}-pe}$ binary variables indicate whether e^ath attack strategy on power plant g in the pre-evaluation stage selected (1) or not (0).

The $y_s^{f^{a}-pe}$ binary variables indicate whether a f^ath attack strategy to substation s in the pre-evaluation stage is selected (1) or not (0).

$x_{sg}^{ef^{a}-pe}$ binary variables indicate whether the e^ath attack strategy to power plant g and the f^ath attack strategy to substation s simultaneously cause a load outage or voltage less than 0.95 to substation s in the pre-evaluation stage selected (1) or not (0).

$xy_g^{\prime ef^{a}-pe}$ Binary variables indicates whether f^ath attack strategy to substation s connected to power plant g and e^ath attack strategy to power plant g simultaneously cause to outage power plant g in pre-evaluation stage selected (0) or not (1)

$xy_s^{\prime ef^{a}-pe}$ Binary variables indicates whether f^ath attack strategy to substation s and e^ath attack strategy to power plant g simultaneously cause to load outage or voltage less than 0.95 to substation s in pre-evaluation stage selected (0) or not (1)

$z_{k,s}^{h^h,f^h}$ Binary variables indicate whether h^hth and f^hth hardening strategies at substations k and s, respectively, are selected (1) or not (0)

$x_g^{e^h}$ Binary variables indicate whether e^hth hardening strategy at power plant g selected (1) or not (0)

$xz_{g,k,s}^{e^h,h^h,f^h}$ Binary variables indicates whether h^hth and f^hth hardening strategy at substation k and s respectively or e^hth hardening strategy at power plant g simultaneously selected (1) or not (0)

$z_{k,s}^{h^a,f^a}$ Binary variables indicate whether h^ath and f^ath attack strategies at substation k and s, respectively, are selected (1) or not (0)

$x_g^{e^a}$ Binary variables indicate whether the e^ath attack strategy at power plant g selected (1) or not (0).

$xz_{g,k,s}^{e^a,h^a,f^a}$ Binary variables indicate whether h^ath and f^ath attack strategy at substations k and s, respectively, or e^ath attack strategy at power plant g simultaneously selected (1) or not (0).

P_g/Q_g Active / Reactive power generation output

P_g^s/Q_g^s Active / Reactive power generation output inject to substation s

P_l^s/Q_l^s Active / Reactive power flow in line l inject to substation s

S_l Apparent power flow in line l

S_s Apparent power injection to substation s

V_s Voltage of substation s

$COVD_g$ Summing the normalized average load interruption cost for 1 hour for different loads due to substations' voltage drop less than 0.95 p.u after attack to power plant g

$CL_k^{h^a}$ Outage critical load with attack to substation k with strategy h^a (MW)

$VD_k^{e^a-g}$ Critical loads with voltage less than 0.95 p.u. in substation k after attack on power plant g with strategy e^a (MW)

LO_s^{ns} Outage load with attack on substation s after construction, ns^{th} new substation to supply loads in substation s in parallel (MW)

VD_s^{g-mg} Loads with voltage less than 0.95 p.u. in substation s after attack to power plant g and construct mg^{th} new power plant due to supply in parallel with power plant g (MW)

$HL_{k,s}^{h^h,f^h}$ Hardened loads in substations k and s with strategies h^h and f^h respectively (MW).

$VD_{k,s}^{e^h-g}$ Loads with voltage more than 0.95 p.u. in substations k and s, respectively, to prevent attack on power plant g after hardening with strategy e^h (MW)

$AL_{k,s}^{h^a,f^a}$ Attacked load in substations k and s with strategies h^a and f^a respectively (MW)

$VD_{k,s}^{e^a-g}$ Loads with voltage less than 0.95 p.u. in substations k and s, respectively, to prevent attack on power plant g after attack with strategy e^a (MW)

REFERENCES

[1] R. Moreno, D. N. Trakas, M. Jamieson, M. Panteli, P. Mancarella, G. Strbac, C. Marnay, and N. Hatziargyriou, "Microgrids against wildfires: Distributed energy resources enhance system resilience," *IEEE Power Energy Mag.*, vol. 20, no. 1, pp. 78–89, Jan. 2022.

[2] *National Security and Assured U.S. Electrical Power*, CNA Mil. Advisory Board, Arlington, VA, USA, Nov. 2015.

[3] *Making the Nation Safer. The Role of Science and Technology in Countering Terrorism*, Nat. Res. Council, Nat. Acad. Press, Washington DC, USA, 2002.

[4] L. Zamparini, "A review of models for transport security and of their relevance for supply chains," *Transp. Rev.*, vol. 25, pp. 1–7, Mar. 2022.

[5] B. Schneier, "Managed security monitoring: Network security for the 21st century," *Comput. Secur.*, vol. 20, no. 6, pp. 491–503, 2001.

[6] V. M. Bier and V. Abhichandani, "Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries," in *Proc. 10th Risk-Based Decisionmaking Water Resour.*, Santa Barbara, CA, USA, Sep. 2003, pp. 59–76.

[7] V. M. Bier, A. Nagaraj, and V. Abhichandani, "Protection of simple series and parallel systems with components of different values," *Rel. Eng. Syst. Saf.*, vol. 87, no. 3, pp. 315–323, Mar. 2005.

[8] Q. Li, M. Li, Z. Gong, Y. Tian, and R. Zhang, "Locating and protecting interdependent facilities to hedge against multiple non-cooperative limited choice attackers," *Rel. Eng. Syst. Saf.*, vol. 223, Jul. 2022, Art. no. 108440.

[9] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat," *IEEE Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[10] B. J. Pierre, D. Krofcheck, K. Munoz-Ramos, and B. Arguello, "A framework to model and analyze electric grid cascading failures to identify critical nodes," in *Proc. 17th Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Jun. 2022, pp. 1–6.

[11] J. Salmeron, K. Wood, and R. Baldick, "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 96–104, Feb. 2009.

[12] G. Levitin, "Optimal defense strategy against intentional attacks," *IEEE Trans. Rel.*, vol. 56, no. 1, pp. 148–157, Mar. 2007.

[13] K. Hausken, "Strategic defense and attack for series and parallel reliability systems," *Eur. J. Oper. Res.*, vol. 186, no. 2, pp. 856–881, Apr. 2008.

[14] K. Hausken, "Strategic defense and attack of complex network," *Int. J. Performability Eng.*, vol. 5, no. 1, pp. 13–30, 2009.

[15] R. Sarkar, "An analytical approach for reducing *k*-line failure analysis and load shed computation," *IET Gener., Transmiss. Distrib.*, vol. 16, no. 13, pp. 2623–2641, 2022.

[16] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, Nov. 2006.

[17] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 4, pp. 712–718, Jul. 2007.

[18] N. Romero, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, "Investment planning for electric power systems under terrorist threat," *IEEE Trans. Power Syst.*, vol. 27, no. 1, pp. 108–116, Feb. 2012.

[19] C. N. Alguacil and S. J. M. Arroyo, "A tri-level programing approach for electric grid defense planning," *Comput. Oper. Res.*, vol. 41, pp. 282–290, Dec. 2014.

[20] W. Yuan, L. Zhao, and B. Zeng, "Optimal power grid protection through a defender–attacker–defender model," *Rel. Eng. Syst. Saf.*, vol. 121, pp. 83–89, Jan. 2014.

[21] W. Yuan and B. Zeng, "Achieving cost-effective power grid hardening through transmission network topology control," Dept. Ind. Manag. Syst. Eng., Univ. South Florida, Tampa, FL, USA, Tech. Rep., Dec. 2014. Accessed: Nov. 23, 2022. [Online]. Available: https://optimization-online.org/?p=13218 and https://optimization-online.org/2014/12/4711/

[22] X. Wu and A. J. Conejo, "An efficient tri-level optimization model for electric grid defense planning," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2984–2994, Jul. 2017.

[23] H. Davarikia and M. Barati, "A tri-level programming model for attack-resilient control of power grids," *J. Modern Power Syst. Clean Energy*, vol. 6, no. 5, pp. 918–929, Sep. 2018.

[24] C. M. Schneider, A. A. Moreira, J. S. Andrade, Jr., S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proc. Nat. Acad. Sci. USA*, vol. 108, no. 10, pp. 3838–3841, Mar. 2011.

[25] L. Ma, M. Gong, Q. Cai, and L. Jiao, "Enhancing community integrity of networks against multilevel targeted attacks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 88, Aug. 2013, Art. no. 022810.

[26] Y. Fang and E. Zio, "Optimizing the resilience of interdependent infrastructure systems against intentional attacks," in *Proc. 2nd Int. Conf. Syst. Rel. Saf. (ICSRS)*, Dec. 2017, pp. 62–67.

[27] C. Wang, W. Wei, J. Wang, F. Liu, F. Qiu, C. M. Correa-Posada, and S. Mei, "Robust defense strategy for gas-electric systems against malicious attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2953–2965, Jul. 2017.

[28] W. Li, Y. Li, Y. Tan, Y. Cao, C. Chen, Y. Cai, K. Y. Lee, and M. Pecht, "Maximizing network resilience against malicious attacks," *Sci. Rep.*, vol. 9, no. 1, Dec. 2019, Art. no. 2261.

[29] H. Karimianfard, H. Haghighat, and B. Zeng, "Co-optimization of battery storage investment and grid expansion in integrated energy systems," *IEEE Syst. J.*, early access, Dec. 30, 2021, doi: 10.1109/JSYST.2021.3130057.

[30] H. Jokar, B. Bahmani-Firouzi, and M. Simab, "Bilevel model for security-constrained and reliability transmission and distribution substation energy management considering large-scale energy storage and demand side management," *Energy Rep.*, vol. 8, pp. 2617–2629, Nov. 2022, doi: 10.1016/j.egyr.2022.01.137.

[31] M. M. Amiri, H. Ameli, M. T. Ameli, and G. Stebac, "Investigating the effective methods in improving the resilience of electricity and gas systems," in *Whole Energy Systems*. Cham, Switzerland: Springer, 2022, pp. 137–152.

[32] M. H. Oboudi, M. Mohammadi, D. N. Trakas, and N. D. Hatziargyriou, "A systematic method for power system hardening to increase resilience against earthquakes," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4970–4979, Dec. 2021, doi: 10.1109/JSYST.2020.3032783.

[33] F. Faramarzi, T. Niknam, J. Aghaie, and M. Rashidi, "Resiliency enhancement of power system against intentional attacks," *IET Renew. Power Gener.*, vol. 16, pp. 3544–3558, 2022, doi: 10.1049/rpg2.12396.

[34] P. J. Balducci, J. M. Roop, L. A. Schienbein, J. G. DeSteese, and M. R. Weimar, "Electric power interruption cost estimates for individual industries, sectors, and the U.S. Economy," Pacific Northwest Nat. Lab., U.S. Dept. Energy, Office Power Technol., Office Distrib. Resour., Richland, WA, USA, Tech. Rep. PNNL-13797, 2002. Accessed: Nov. 23, 2022. [Online]. Available: https://www.pnnl.gov/main/publications/external/technical_reports/pnnl-13797.pdf

[35] R. D. Zimmerman and C. E. Murillo-Sánchez. *MATPOWER: A MATLAB Power System Simulation Package*. Accessed: Mar. 21, 2015. [Online]. Available: http://www.pserc.cornell.edu/matpower

[36] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 9–12, Jun. 2011.

[37] Christie. (Aug. 1993). *Power Systems Test Case Archive*. Accessed: Feb. 4, 2015. [Online]. Available: http://www.ee.washington.edu/research/pstca/pf30/pg_tca30bus.htm

[38] R. Gnanadass, "Optimal power dispatch and pricing for deregulated power industry," Ph.D. dissertation, Dept. Electron. Commun. Eng., Pondicherry Univ., Pondicherry, India, Mar. 2005. Accessed: Mar. 22, 2015. [Online]. Available: http://dspace.pondiuni.edu.in/jspui/bitstream/pdy/498/1/T3248.pdf

[39] M. Shahidehpour and Y. Wang, *Communication and Control in Electric Payer Systems: Application of Parallel and Distributed Processing*. Piscataway, NJ, USA: Wiley, 2003.

[40] *On Unit Investment Cost Indicators and Corresponding Reference Values for Electricity and Gas Infrastructure*, Univ. Illinois Chicago, Chicago, IL, USA, 2015.

[41] *Security Guards Cost*. Accessed: Nov. 23, 2022. [Online]. Available: https://www.thumbtack.com/p/security-guards-cost

FARSHAD FARAMARZI was born in Shiraz, Fars, Iran, in 1969. He received the B.S. degree in electrical engineering from Shiraz University, Shiraz, in 1993, and the M.S. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 1998. His research interests include power system operation, resiliency, optimization, and planning.

TAHER NIKNAM (Member, IEEE) was born in Shiraz, Iran. He received the B.S. and M.S. degrees from Shiraz University and the Ph.D. degree from the Sharif University of Technology. He is currently a Faculty Member of the Electrical Engineering Department, Shiraz University of Technology. His research interests include power system restructuring, the impact of distributed generation on power systems, optimization methods, and evolutionary algorithms.

MOTAHAREH POURBEHZADI (Member, IEEE) received the Ph.D. degree from the Shiraz University of Technology, in 2021. She is currently pursuing the Ph.D. degree in big data analytics with the Muma College of Business, University of South Florida. She has also been a Researcher and a Data Scientist at the University of South Florida, since 2019. Her research interests include optimization, machine learning, security, and privacy of big data systems and healthcare analytics. She is among the top ten reviewers of the ISTE journal and serves as a Reviewer for the IEEE Transactions on Industry Applications.

GITI JAVIDI (Member, IEEE) received the B.S. degree from the University of Central Oklahoma and the M.S. and Ph.D. degrees from the University of South Florida. She is currently working as a Faculty Member of the University of South Florida. Her research interests include human–computer interaction, data visualization, and STEM education. She has been involved in computer science and research in this area for 16 years. She has a long list of publications and research grants, including projects with NASA, NSF, MSIP, and industry partners.

EHSAN SHEYBANI (Senior Member, IEEE) received the B.S. degree in electrical engineering from UF, the M.S. degree in electrical engineering from FSU, and the Ph.D. degree in electrical engineering from USF. He is currently a Faculty Member of the University of South Florida. His primary research interests include communication, signal processing, and data analysis. He has been involved in teaching, practicing, researching, and consulting DSP applications in technology, systems analysis, and data science for the past 20 years. He has a long list of publications and research grants, including projects with NASA, NSF, NIH, DoD, DEd, and industry partners.