Electric Power Systems Research 143 (2017) 329–338

Contents lists available at ScienceDirect

Electric Power Systems Research

journal homepage: www.elsevier.com/locate/epsr

A risk optimization model for enhanced power grid resilience against physical attacks

Nasim Nezamoddini [a], Seyedamirabbas Mousavian [b,*], Melike Erol-Kantarci [c]

[a] The Department of Industrial and Systems Engineering, State University of New York, Binghamton, NY, USA
[b] The School of Business, Clarkson University, Potsdam, NY, USA
[c] The School of Electrical Engineering and Computer Science, University of Ottawa, ON, Canada

ARTICLE INFO

Article history:
Received 14 February 2016
Received in revised form 17 August 2016
Accepted 18 August 2016
Available online 25 October 2016

Keywords:
Transmission system security
Physical attacks
Load curtailment/shed
Mixed integer linear programming

ABSTRACT

Secure operation of the power systems is a major concern of the power system operators, consumers and governments. Besides inevitable malfunction of the power grid components, deliberate disruptions caused by malicious attacks put the security of the power systems at high risk. Transmission systems have been targeted by attackers to interdict the supply of power to consumers. In this paper, we address the problem of the transmission system security and develop an optimization model to determine the optimal investment decision for the resilient design of the transmission systems against physical attacks. We measure the damage of the physical attacks in terms of the load curtailment. We model the optimal protection decision problem as a mixed integer linear programming (MILP) problem to minimize the investment costs such that the risk of the load curtailment exceeding a certain threshold value, after an attack to the power grid, be less than the risk tolerance value, defined by power system operators. We use the small 6-bus test system to describe the problem and our methodology. We run our experiments on the IEEE 24-bus and IEEE 57-bus systems to test the performance of our model. Experimental results show that the developed model is a promising enhancement to ensure secure and safe operation of the transmission systems.

1. Introduction

Power grids are indispensable components of modern life. The safe and secure operation of the power grid is of the highest priority for power grid operators, consumers and government. However, disruptions in power supply are sometimes inevitable due to the malfunction of the power grid components and environmental issues [1]. As a case in point, weather related power outages in the United States cost $18–$33 billion in annual average between 2003 and 2012 [2]. Deliberate disruptions, caused by malicious attacks to the power grids, are major concerns for the power grid stakeholders as well. Malicious attacks to power grids not only cause disruption in power supply but also lead to substantial economic burdens for the utility companies. For example, the recent attack to the substation in California on April 16, 2013 resulted in damaging 17 giant transformers and 27 days of repair time [3]. A report from Wall Street Journal showed that 274 instances of deliberate damages to the power grid were reported over the last three years, which put more emphasis on necessity of enhanced protection and resilience of the power grid [4]. However, substantial protection costs preclude the full protection of all grid components and encourage power system investors to investigate critical components of the system for enhanced security [5]. Damages to the critical power grid components may entail cascading outages and cause blackouts [6]. Hence, a risk assessment model is necessary to determine potential vulnerabilities of the power grid and provide the system operators with enhanced protection plans within the budgetary restrictions.

Due to the statistics mentioned above, the problem of power grid resilience against physical attacks has attracted the interests of the research community as well. The main objective is to determine the best investment policy for protecting the power grid components against physical attacks where the attacker's resources are limited [7]. The interdiction attacks cause topological changes to the power grid which impact is measured in terms of the load shed [8]. Authors in [9] developed a multi-level optimization problem in the form of defender-attacker-defender to identify the critical components necessary to be hardened for minimizing the potential damages of the terrorist attacks. Multi-level optimization problems

* Corresponding author.
E-mail addresses: nnezamo1@binghamton.edu (N. Nezamoddini), amir@clarkson.edu (S. Mousavian), melike.erolkantarci@uottawa.ca (M. Erol-Kantarci).

http://dx.doi.org/10.1016/j.epsr.2016.08.046
0378-7796/

Nomenclature

Sets and indices

K	set of buses
G	set of generators
L	set of transmission lines
I	set of protection levels
Φ	set of attack scenarios
k	index of buses
g	index of generators
l	index of transmission lines
i	index of protection levels
ϕ	index of attack scenarios

Constants

C_i	cost of the protection level i
R_i	reliability of the protection level i
L_k	load of bus k (MW)
S_l	susceptance of transmission line l (siemens)
$\delta_{\phi l}$	binary parameter which equals 1 if transmission line l is interdicted in scenario ϕ, and 0 otherwise
H_{lk}	incidence matrix coefficient (−1, 0 or 1) at bus k of transmission line l
$p_g^{\max}$	maximum generation of generator g (MW)
$p_g^{\min}$	minimum generation of generator g (MW)
$f_l^{\max}$	maximum capacity of transmission line l (MVA)
ψ	threshold of the load curtailment (MW)
ϵ	risk tolerance value of the threshold load curtailment
N	attacker's budget in terms of the number of transmission lines interdicted

Decision variables

x_{il}	binary decision variable which equals 1 if transmission line l is equipped with protection level i, and 0 otherwise
w_ϕ	binary decision variable which equals 1 if the load curtailment exceeds the threshold in scenario ϕ, and 0 otherwise
$p_{\phi g}$	energy dispatched by generator g in scenario ϕ. (MW)
$f_{\phi l}$	power flow at transmission line l in scenario ϕ (MVA)
$\eta_{\phi k}$	load curtailment of bus k in scenario ϕ. (MW)
$\theta_{\phi\alpha(l)}$	voltage angle at the from-bus end of the transmission line l in scenario ϕ (°)
$\theta_{\phi\beta(l)}$	voltage angle at the to-bus end of the transmission line l in scenario ϕ (°)
P_ϕ	probability of the attack success in scenario ϕ

are complicated. A bilevel optimization problem can be converted to a single level optimization problem using Karush–Kuhn–Tucker optimality conditions [10]. Authors in [11] showed that decomposition methods can be applied effectively to solve large scale bilevel protection models. Iterative heuristics are also proposed to solve such complex optimization problems [12]. Computational time in such problems is of the interests of the research community as well [13,14]. Game theory models are introduced in [15] to tackle the defender-attacker problems. The application of game theory models in defender-attacker problems have been further studied in [16] as static games and in [17] as leader-follower games. zero-sum Markov games in [18] and graph theory based methods in [19–21] are introduced to solve the power grid interdiction problem. Furthermore, transmission switching has been suggested as a corrective action when the power grid is attacked [22]. Authors in [23] applied meta-heuristic methods to solve the interdiction model with the possibility of transmission switching. The mentioned defender-attacker models aim at hardening the power grid against the worst potential attack scenarios. Besides, the underlying assumption of the interdiction models is that the protected components will no longer be at risk and completely secure. However, it is not a realistic assumption. To alleviate this problem, we define a protection reliability index which represents the probability that the protection mechanism can keep the transmission line active even after malicious attacks. In other words, protection reliability index represents the likelihood of the attacker's failure in harming the transmission line due to the protection mechanisms placed in service. Besides, there are situations where decision makers prefer to equip some grid components with partial protections due to the substantial protection costs. After a comprehensive review, the author in [24] concluded that it has been difficult in power systems studies to relate reliability and resiliency to market efficiency and economic losses. Hence, we propose a new model for power grid protection, which provides power system operators with more flexibility in terms of the resiliency scales against the risk of malicious attacks. Various line protection techniques are introduced in [25] that incur different costs for utility companies. For example, intrusion detection devices, access controls, lighting, fencing, cameras, sensors, and buffer zone security are suggested as protection mechanisms [26] with lower reliability and small to medium cost investments. Moreover, more reliable protection mechanisms such as undergrounding or double circuiting of the transmission lines can be used at higher costs to enhance physical security against physical disruptions [27]. A communication mechanism can also be devised to alarm guards/police to accelerate the response time to intrusions [28]. Hence, we consider the possibility of different protection levels and study risk in our model formulation as a decision parameter where the protected components are less likely to be tampered by attackers.

2. Protection optimization model

This paper aims at developing a protection model to equip critical components of the transmission systems with more reliable protections. Attackers may target the physical structure of the power grid such as transmission lines, transmission towers or insulators [28]. These attacks incapacitate the entire transmission line and cause insufficient available transmission capacity that eventually interrupt the balance between power supply and demand. Therefore, control actions such as load curtailment/shedding need to be taken after an attack in order to stabilize the system [29]. Load curtailment reduces lower-priority loads with the permission of the customers; in case curtailment is not sufficient to prevent power imbalance or there is not enough time to implement the load curtailment, load will be shed [30]. The goal of this paper is to minimize the investment costs of protection such that the risk of load curtailment/shedding exceeding a certain threshold value would be controlled. The assumptions of our proposed model are as follows.

- There are potential protection mechanism which provide transmission lines with different reliability levels at different costs.
- Attackers have limited budgets to tamper with the system.
- Attackers do not have complete information about the protections plans.
- The risks are calculated in terms of total load curtailment.

The objective function of our mathematical model, given in Eq. (1), is to minimize the investment costs of equipping the transmission lines with more reliable protections:

$$Z = \min_{\mathbf{x}} \sum_{l=1}^{L} \sum_{i=1}^{I} C_i x_{li} \tag{1}$$

where C_i is the cost of the protection level i and x_{il} is the binary decision variable which equals 1 if transmission line l is equipped with protection level i, and 0 otherwise.

We consider that attackers have limited budget to tamper with the transmission lines. The attackers' budget is represented in Eq. (2):

$$\sum_{l=1}^{L} \delta_{\phi l} = N \quad \forall \phi \in \Phi \tag{2}$$

where $\delta_{\phi l}$ is a binary input parameter that equals to one if the transmission line is interdicted and 0 otherwise. The attacker's total budget is represented by parameter N.

The goal is to find the optimal investment plan such that the load curtailment would be controlled under all potential attack scenarios. We use the linearized optimal power flow constraints, known as DC-OPF constraints [31,32], and modify them as follows such that the attack scenarios and load curtailment are integrated in the model. Notice that L_k represents the peak load to ensure that the model considers worst cases when the slightest attacks may result in load curtailment:

$$\sum_{l=1}^{L} H_{lk} f_{\phi l}(1 - \delta_{\phi l}) + p_{\phi k} + \eta_{\phi k} = L_k \quad \forall k \in K; \quad \forall \phi \in \Phi \tag{3}$$

Eq. (3) is the load balance constraint where H_{lk} is the incidence matrix coefficient (−1, 0 or 1) at bus k of transmission line l, $p_{\phi g}$ represents energy dispatched by generator g in scenario ϕ and $f_{\phi l}$ determines the power flow at transmission line l in scenario ϕ. In Eq. (3), interdicted lines by the attacker are excluded from the list of connected transmission lines when $\delta_{\phi l} = 1$. Moreover, the load curtailment stem from the attack is obtained by $\eta_{\phi k}$ at bus k. Eqs. (4) and (5) represent the voltage angles and the power flows constraints in the modified DC-OPF. Notice that $\theta_{\phi\alpha(l)}$ and $\theta_{\phi\beta(l)}$ represent voltage angle at the from-bus end and the to-bus end of the transmission line l in scenario ϕ, respectively, and S_l is the susceptance of transmission line l.

$$f_{\phi l} - S_l(\theta_{\phi\alpha(l)} - \theta_{\phi\beta(l)}) \geq -M\delta_{\phi l} \quad \forall l \in L; \quad \forall \phi \in \Phi \tag{4}$$

$$f_{\phi l} - S_l(\theta_{\phi\alpha(l)} - \theta_{\phi\beta(l)}) \leq M\delta_{\phi l} \quad \forall l \in L; \quad \forall \phi \in \Phi \tag{5}$$

We used the big-M parameter, M, to exclude the voltage angles and power flow constraint from the model for the transmission line that is interdicted, $\delta_{\phi l} = 1$. Eqs. (6) and (7) represent the constraints on the capacities of the transmission lines and generators:

$$-f_l^{\max}(1 - \delta_{\phi l}) \leq f_{\phi l} \leq f_l^{\max}(1 - \delta_{\phi l}) \quad \forall l \in L; \quad \forall \phi \in \Phi \tag{6}$$

$$p_g^{\min} \leq p_{\phi g} \leq p_g^{\max} \quad \forall g \in G; \quad \forall \phi \in \Phi \tag{7}$$

Eq. (8) is provided to ensure that the load curtailment at each bus does not exceed the load of the bus.

$$0 \leq \eta_{\phi k} \leq L_k \quad \forall \phi \in \Phi; \forall k \in K \tag{8}$$

There are potential levels of protection which provide transmission lines with different protection reliability at different costs. A transmission line will be protected by only one of the protection mechanisms or will be left unprotected as given in Eq. (9). In Eq. (9), x_{li} is a binary variable that determines line l is protected by protection type i. Notice that $x_{l0} = 1$ means that line l is not protected and $C_0 = 0$ accordingly:

$$\sum_{i=1}^{I} x_{li} = 1 \quad \forall l \in L \tag{9}$$

The goal of the proposed model is to ensure that the obtained protection plan guarantees that the risk of the load curtailment exceeding a certain threshold would be less than a predetermined acceptable risk tolerance value, e.g. the risk of the load curtailment exceeding 10 MW would be less than 1% considering all potential attack scenarios. The risk constraint is given in Eq. (10):

$$Pr\left(\sum_{k=1}^{K} \eta_{\phi k} \geq \psi\right) \leq \epsilon \quad \forall \phi \in \Phi \tag{10}$$

where ψ is the load curtailment threshold after the attack from the power system operators' standpoint and ϵ is the acceptable risk tolerance value. To represent Eq. (10) in a linear fashion, we use the binary variable w_ϕ with the definition given in Eq. (11):

$$w_\phi = \begin{cases} 1 & \sum_{k=1}^{K} \eta_{\phi k} \geq \psi \\ 0 & \sum_{k=1}^{K} \eta_{\phi k} < \psi \end{cases} \quad \forall \phi \in \Phi \tag{11}$$

Furthermore, Eq. (12) is considered to ensure that the risk of the load curtailment exceeding a certain threshold value is less than the predetermined acceptable risk value, ϵ:

$$P_\phi w_\phi \leq \epsilon \quad \forall \phi \in \Phi \tag{12}$$

where P_ϕ is the probability of the successful attack in scenario ϕ. Eq. (13) shows how the scenario probabilities are calculated where R_i is the reliability index of the protection type i. The protection reliability index represents the probability that the transmission line remains functional after a malicious attack due to the protection mechanisms placed in service:

$$P_\phi = \prod_{l=1}^{L} \sum_{i=1}^{I} x_{li}(1 - R_i)\delta_{\phi l} \quad \forall \phi \in \Phi \tag{13}$$

Eq. (13) is nonlinear which makes Eq. (12) nonlinear as well. To represent Eq. (13) in a linear fashion, we use variable $u_\phi = \ln P_\phi$. Hence, we obtain Eq. (14) which is still nonlinear:

$$u_\phi = \sum_{l=1}^{L} \ln\left(\sum_{i=1}^{I} x_{li}(1 - R_i)\delta_{\phi l}\right) \quad \forall \phi \in \Phi \tag{14}$$

Considering variable x_{li} being binary, we can obtain the equivalent linear Eq. (15):

$$u_\phi = \sum_{l=1}^{L} \sum_{i=1}^{I} x_{li}\delta_{\phi l} \ln((1 - R_i)) \quad \forall \phi \in \Phi \tag{15}$$

Now, we are able to represent Eq. (12) linearly by using Eqs. (16)–(18):

$$\psi . w_\phi - M(1 - w_\phi) \leq \sum_{k=1}^{K} \eta_{\phi k} \quad \forall \phi \in \Phi \tag{16}$$

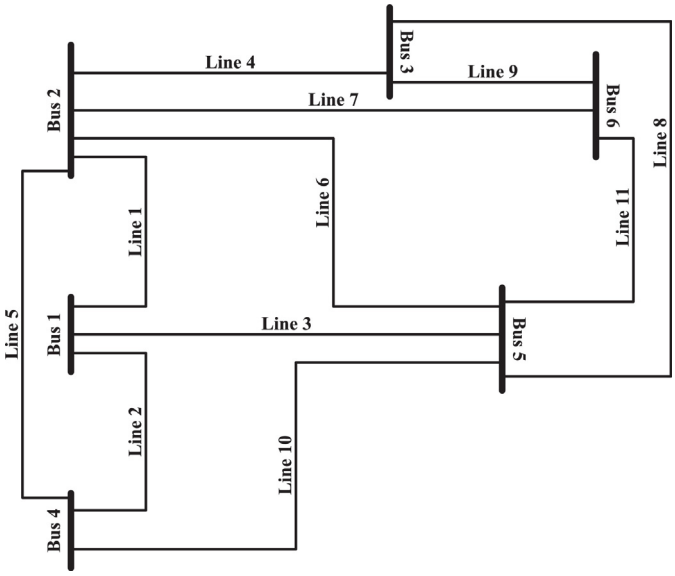

Fig. 1. The 6-bus test system.

$$\sum_{k=1}^{K} \eta_{\phi k} < \psi(1 - w_\phi) + M w_\phi \quad \forall \phi \in \Phi \tag{17}$$

$$u_\phi \leq \ln(\epsilon) + M(1 - w_\phi) \quad \forall \phi \in \Phi \tag{18}$$

Finally, Eq. (19) shows that the decision variables x_{li} are binary:

$$x_{li} \in \{0, 1\} \quad \forall l \in L; \quad \forall i \in I \tag{19}$$

3. Case study and scenario reduction strategy

In this section, we use the 6-bus test system introduced in [31] to describe the problem and our methodology on a small and simple power system. Next, we explain our scenario reduction strategy for larger power systems. We test the efficacy of our approach in the experimental results section using a middle size and a larger power systems.

3.1. Case study

The 6-bus test system includes six buses, three generators and eleven transmission lines. Fig. 1 shows the 6-bus test system. Load profile is given in Table 1. Table 2 shows the reliability levels and investment costs of the four assumed protection mechanisms. The reliability level of Mechanism 0, no enhanced protection of the transmission lines, is assumed to be 0.50. Besides, it is assumed that the attacker's budget is limited and may target two transmission lines at most. Hence, all single-line and two-line attack scenarios are enumerated and resulting load curtailments are calculated and summarized in Table 3.

Table 1
Load in the 6-bus test system (MW).

Bus	1	2	3	4	5	6
Load	0	0	0	70	70	70

Table 2
Reliability levels and costs of the protection mechanisms.

Protection level	0	1	2	3
Protection reliability	0.5	0.8	0.9	0.99
Cost (p.u.)	0	1	2	3

Table 3
Load curtailments of the single-line and two-line attack scenarios.

Scenario #	Attacked lines	Load curtailment (MW)
1	Single line	0
2	2, 3	6.25
3	2, 5	50.00
4	2, 6	1.81
5	2, 8	8.09
6	2, 9	2.97
7	2, 10	10.00
8	2, 11	1.03
9	3, 8	3.00
10	5, 8	0.57
11	5, 10	10.00
12	7, 9	30.00
13	Other 2-lines combinations	0

First, we explore how the 6-bus test system should be protected considering different risk tolerance values if the threshold of the load curtailment is 40 MW, $\psi = 40$. Therefore, the model is supposed to protect the system against Scenario 3, introduced in Table 3, such that the probability of that scenario be less than or equal to the risk tolerance value. In this experiment, we analyze the impact of risk tolerance values ranging from 0.001 to 0.500 on protection plans. The results are summarized in Table 4 and show that risk averse protection plans increase investment costs substantially and require more number of higher-reliability protection mechanisms to be installed.

Next, we run an experiment to study the impact of the load curtailment threshold value on the resultant protection plans. The results, summarized in Table 5, show that lower threshold values necessitate protection of more number of transmission lines. The reason is that more attack scenarios are effective when the threshold is set to lower values. To test the validity of our obtained solutions, we calculated the probabilities of the attack scenarios after the protection plan, given in Table 5, is implemented for $\psi = 0$ and $\epsilon = 0.01$. We summarized the results in Table 6 which confirms that the probability of load curtailment under any attack scenario is equal to or less than the risk tolerance value.

To study the impact of costs, we compare the protection plans under the two cost profiles, provided in Table 7. The protection decisions for the two mentioned cost profiles are given in Table 8 when $\psi = 0$ and $\epsilon = 0.01$. The results show that the protection plans are very sensitive to the relative cost ratio of the protection mechanisms. Moreover, the scenario probabilities under the two given protection decisions are compared in Table 9. The results confirm that the protection costs may change the protection decisions significantly while satisfying the risk constraints.

Table 4
Impact of risk tolerance value on protection plans.

Risk (ϵ)	(l: protected line, i: protection level)	Total cost (p.u.)
0.500	–	0
0.100	(2,1)	1
0.050	(2,2)	2
0.010	(2,3)	3
0.001	(2,3),(5,2)	5

Table 5
Protection plans for different load curtailment threshold values at $\epsilon = 0.01$.

ψ	(l: protected line, i: protection level)	Total cost
0	(2,3),(5,3),(8,3),(9,3)	12
10	(2,3),(7,3),(10,3)	9
30	(2,3),(7,3)	6
50	(2,3)	3
>50	–	0

Table 6
Scenario probabilities.

Scenario attacked lines	Load curtailment (MW)	Probability after protection
2, 3	6.25	0.0100
2, 5	50.00	0.0001
2, 6	1.81	0.0100
2, 8	8.09	0.0001
2, 9	2.97	0.0001
2, 10	10.00	0.0100
2, 11	1.03	0.0100
3, 8	3.00	0.0100
5, 8	0.57	0.0001
5, 10	10.00	0.0100
7, 9	30.00	0.0100

Table 7
Protection costs.

Protection level	0	1	2	3
Protection reliability	0.5	0.8	0.9	0.99
Cost plan #1 (p.u.)	0	1	2	3
Cost plan #2 (p.u.)	0	1	1.25	3

Table 8
Cost impact on protection decisions at $\psi = 0$ and $\epsilon = 0.01$.

Cost plan	(l: protected line, i: protection level)
#1	(2,3),(5,3),(8,3),(9,3)
#2	(2,3),(3,2),(5,2),(7,2),(8,2),(9,2),(10,2)

Table 9
Scenario probabilities of the two cost profiles.

Scenario attacked lines	Load curtailment (MW)	Probability cost #1	Probability cost #2
2, 3	6.25	0.0100	0.0010
2, 5	50.00	0.0001	0.0010
2, 6	1.81	0.0100	0.0100
2, 8	8.09	0.0001	0.0010
2, 9	2.97	0.0001	0.0010
2, 10	10.00	0.0100	0.0010
2, 11	1.03	0.0100	0.0100
3, 8	3.00	0.0100	0.0100
5, 8	0.57	0.0001	0.0100
5, 10	10.00	0.0100	0.0100
7, 9	30.00	0.0100	0.0100

Finally, we study the impact of the attacker's budget on protection plans. In this experiment, we assume $\epsilon = 0.001$ and $\psi = 40$ whereas the attacker's budget varies between 1 and 3 transmission lines. The results, summarized in Table 10, show that the investment cost increases as the attacker's budget increases. As a case in point, the investment cost increases by 80% when the attacker's budget is increased from two lines to three lines. The reason is that the attacks are more severe and the system investors need to equip more number of transmission lines with enhanced protections to secure the safe operations of the power grid.

3.2. Scenario reduction strategy

In the case study, we enumerated all attack scenarios and obtained the load curtailments to describe the problem and our methodology. Our model included all potential attack scenarios for the 6-bus test system to obtain the optimal protection decisions. We were able to include all scenarios since the test system was small. However, it is not possible to enumerate and include all potential scenarios for large systems since it is known that MILP solvers suffer from the curse of dimensionality. Therefore, we need to reduce the number of potential scenarios to handle larger power systems.

Table 10
Impact of attacker's budget on protection plans.

Attacker's budget	(l: protected line, i: protection level)	Total cost (p.u.)
1	–	0
2	(2,3),(5,2)	5
3	(2,3),(5,2),(7,1),(9,3)	9

Table 11
Load profile of the IEEE 24-bus system.

Bus	Load (MW)	Bus	Load (MW)
1	108	13	265
2	97	14	194
3	180	15	317
4	74	16	100
5	71	17	0
6	136	18	333
7	125	19	181
8	171	20	128
9	175	21	0
10	195	22	0
11	0	23	0
12	0	24	0

Our strategy to reduce the number of potential scenarios is based on two principals. First, it is more likely that the attack damages are more severe if the attackers target the transmission lines in the same neighborhood. Therefore, we consider the incident transmission lines of a bus and those of its adjacent buses a neighborhood. Secondly, it is likely that the attacker attempts to form an island by attacking N transmission lines assuming that the attacker has the knowledge of the structure of the system. Islands could happen when a series of buses are connected and those buses are adjacent to less than N buses. Thus, we consider the incident transmission lines to these connected buses a special neighborhood as well. Next, we find all combinations of 1, 2, .. ., N transmission lines in each neighborhood to form the list of the potential scenarios and remove the repeated scenarios from the list.

4. Experimental results

To show the efficacy of our model in larger power systems and the importance of the scenario reduction strategy, we test the performance of our proposed protection optimization model on the IEEE 24-bus and IEEE 57-bus test systems introduced in [33].

4.1. 24-Bus test system

The IEEE 24-bus test system consists of 38 transmission lines, 24 buses and 33 generators. The IEEE 24-bus test system is shown in Fig. 2. The load profile is given in Table 11 and the protection levels are as provided in Table 2. We refer the readers to [33,32] for additional systems data.

We set the threshold value to 50 MW and the risk tolerance value to 0.01. We assume that the attacker may target three transmission lines at most simultaneously. Therefore, the total number of potential attack scenarios is 9177 scenarios including attacks to 1, 2 and 3 transmission lines. The number of attack scenarios is reduced to 2513 by applying the proposed scenario reduction strategy, which accounts for 73% reduction in total number of scenarios. The optimal protection decision is obtained and provided in Table 12.

To show the efficacy of our model, we enumerated all attack scenarios and obtained the load curtailments, which took more than 12 h CPU time. The attack scenarios that result in load curtailment, their load curtailments and corresponding probabilities after implementing the protection plan, given in Table 12, are listed in

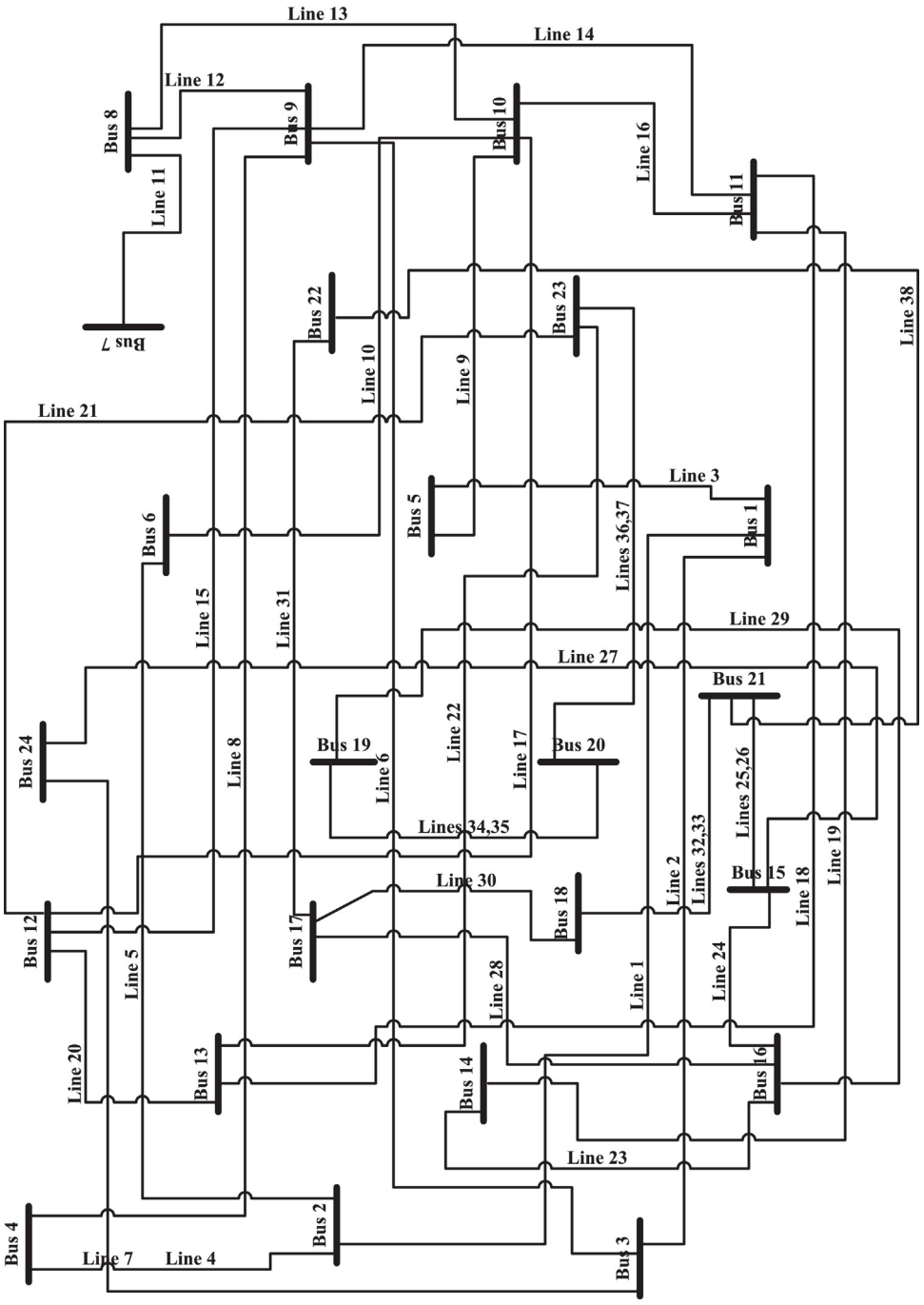

Fig. 2. The IEEE 24-bus test system.

Table 12
Protection decision at $\psi = 50$ MW and $\epsilon = 0.01$.

(l: protected line, i: protection level)	Total cost
(2,3),(4,3),(9,3),(10,3),(11,1),(12,1) (13,1),(23,3),(28,3),(29,3)	24

Table 13. Notice that attack scenarios in which load curtailment is under the threshold value are marked with an asterisk and could have a probability greater than the risk tolerance value.

Next, we show the protection decision when the power system operators are more conservative and set the threshold value to zero, $\psi = 0$. The results are provided in Table 14.

Next, we study the effect of threshold value on protection plans in the IEEE 24-bus test system. The risk tolerance value is set to 0.01, $\epsilon = 0.01$, in the experiment whereas the threshold value, ψ, varies between 0 and 250 MW. The protection plans are summarized in Table 15. The results show that lower threshold values necessitate protection of more number of transmission lines as well as more utilizing more number of higher-reliability protection mechanisms.

Furthermore, we analyze the impact of the reliability level of the no-protection level on the optimal decision. Assuming $\psi = 0$ MW and $\epsilon = 0.01$, we find the optimal protection cost where R_1 varies between 0.05, . . ., 0.79. The results are summarized in Fig. 3. Notice that the optimal decision is not sensitive to the reliability of the no-protection level, R_1, when it is less than 0.68.

Table 13
Load curtailment under the attack scenarios for the IEEE 24-bus test system.

Scenario #	Attacked lines	Load curtailment (MW)	Probability
1	3, 9	71	0.00500
2	4, 8	74	0.00500
3	5, 10	136	0.00500
4	19, 23	194	0.00500
5*	1, 4, 10	41	0.00005
6	1, 8, 10	115	0.00250
7	2, 6, 7	180	0.00250
8	2, 6, 27	180	0.00250
9	7, 23, 29	165	0.00005
10	7, 24, 28	110	0.00250
11	11, 12, 13	171	0.00800
12*	11, 16, 17	18.1	0.05000
13*	12, 16, 17	11.5	0.05000
14*	13, 16, 17	14.5	0.05000
15*	21, 22, 23	24	0.00250
16	23, 27, 29	165	0.00005
17	24, 27, 28	110	0.00250
18	25, 26, 28	212	0.00250
19	29, 34, 35	181	0.00250
20	29, 36, 37	309	0.00250

Table 14
Protection decision at $\psi = 0$ MW.

ϵ	(l: protected line, i: protection level)	Total cost
0.001	(2,1),(3,3),(4,3),(5,2),(6,3),(8,2),(9,2) (10,3),(12,1)(13,3),(16,1),(17,3) (19,2),(21,1),(23,3),(24,1),(25,1) (28,3),(29,3),(35,1),(37,1),	43
0.01	(2,3),(8,3),(9,3),(10,3),(11,1),(12,1),(13,1) (16,1),(17,1)(23,3),(28,3),(29,3)	26
0.05	(3,1),(4,1),(5,1),(6,1),(8,1),(9,1),(10,1) (13,1),(17,1)(19,1),(23,1),(28,1),(29,1)	13
0.10	(2,1),(3,1),(4,1),(10,1),(13,1) (16,1),(23,1),(28,1),(29,1)	9

Table 15
Protection decision at $\epsilon = 0.01$.

ψ	(l: protected line, i: protection level)	Total cost
0	(2,3),(8,3),(9,3),(10,3),(11,1),(12,1),(13,1) (16,1),(17,1)(23,3),(28,3),(29,3)	26
50	(2,3),(4,3),(9,3),(10,3),(11,1),(12,1) (13,1),(23,3),(28,3),(29,3)	24
100	(2,3),(10,3),(11,1),(12,1),(13,1) (23,3),(28,3),(29,3)	18
150	(2,3),(11,1),(12,1),(13,1),(23,3) (25,1),(26,1),(28,1),(29,3)	15
200	(26,2),(28,1),(29,3)	6
250	(36,3)	3

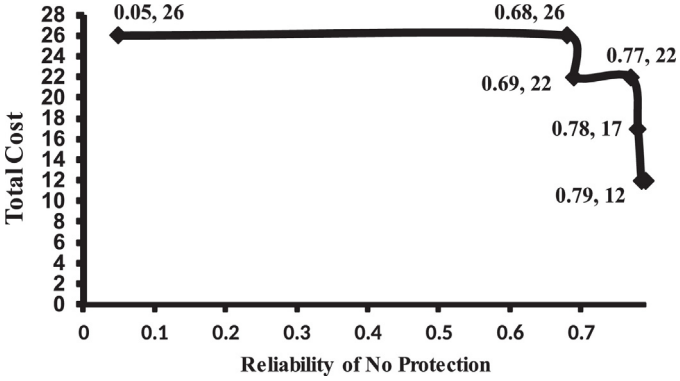

Fig. 3. The effect of the reliability of the no-protection level on optimal protection decision.

Table 16
Load profile of the IEEE 57-bus system.

Bus	Load (MW)	Bus	Load (MW)	Bus	Load (MW)
1	55	20	2.3	39	0
2	3	21	0	40	0
3	41	22	0	41	6.3
4	0	23	6.3	42	7.1
5	13	24	0	43	2
6	75	25	6.3	44	12
7	0	26	0	45	0
8	150	27	9.3	46	0
9	121	28	4.6	47	29.7
10	5	29	17	48	0
11	0	30	3.6	49	18
12	377	31	5.8	50	21
13	18	32	1.6	51	18
14	10.5	33	0	52	4.9
15	22	34	0	53	20
16	43	35	6	54	4.1
17	42	36	0	55	6.8
18	27.2	37	0	56	7.6
19	3.3	38	14	57	6.7

4.2. 57-Bus test system

The IEEE 57-bus test system consists of 80 transmission lines, 57 buses and 7 generators. Fig. 4 shows the IEEE 57-bus test systems. The load profile is given in Table 16 and the protection levels are as provided in Table 2. We refer the readers to [33,32] for additional systems data.

We set the risk tolerance value to 0.01 and assume that the attacker may target three transmission lines at most simultaneously. Therefore, the total number of potential attack scenarios is 85, 400 scenarios including attacks to 1, 2 and 3 transmission lines. The number of attack scenarios is reduced to 8612 by applying the proposed scenario reduction strategy, which accounts for 90% reduction in the total number of scenarios. The optimal protection decision considering the scenario reduction strategy is provided in Table 17.

Furthermore, we show the protection decision when the power system operators conservatively set the threshold value to zero, $\psi = 0$. The results are summarized in Table 18. The results confirm that conservative designs necessitate higher reliability protections

Table 17
Protection decision at $\epsilon = 0.01$.

ψ	(l: protected line, i: protection level)	Total cost
70	–	0
60	(80,3)	3
50	(41,3)	3
40	(13,1),(16,3),(17,3),(28,1),(33,1) (40,2),(41,3),(48,2),(61,1),(63,3)	20
30	(13,1),(16,3),(17,3),(19,3),(28,1),(33,3) (34,3),(41,3),(45,3),(61,1),(63,3),(80,3)	30
20	(16,3),(17,3),(20,3),(33,3),(34,3),(35,2) (36,1),(41,3),(42,3),(60,1),(61,3),(62,1), (63,3),(64,3),(67,3),(68,3),(79,1)	42
10	(4,3),(16,3),(17,3),(19,1),(20,2),(28,1) (29,1),(33,1),(34,1),(36,1),(40,3),(41,1) (42,2),(43,2),(44,2),(45,3),(46,2),(47,2) (48,2),(49,1),(53,1), (57,3),(59,2),(60,2) (61,2),(62,1),(63,3),(64,3),(67,2),(68,2) (69,2),(70,2),(80,2)	64
0	(4,3),(16,3),(17,3),(19,1),(23,1),(28,1) (29,2),(30,2),(31,2),(32,2),(34,3),(35,1) (37,2),(38,2),(39,2),(40,2),(42,2),(43,2) (44,2),(46,2),(47,2),(48,2),(49,2),(55,3) (56,3),(57,3),(59,2),(60,2),(61,2),(63,2) (64,2),(65,2),(67,2),(68,2),(69,2),(70,2) (77,3),(80,2)	80

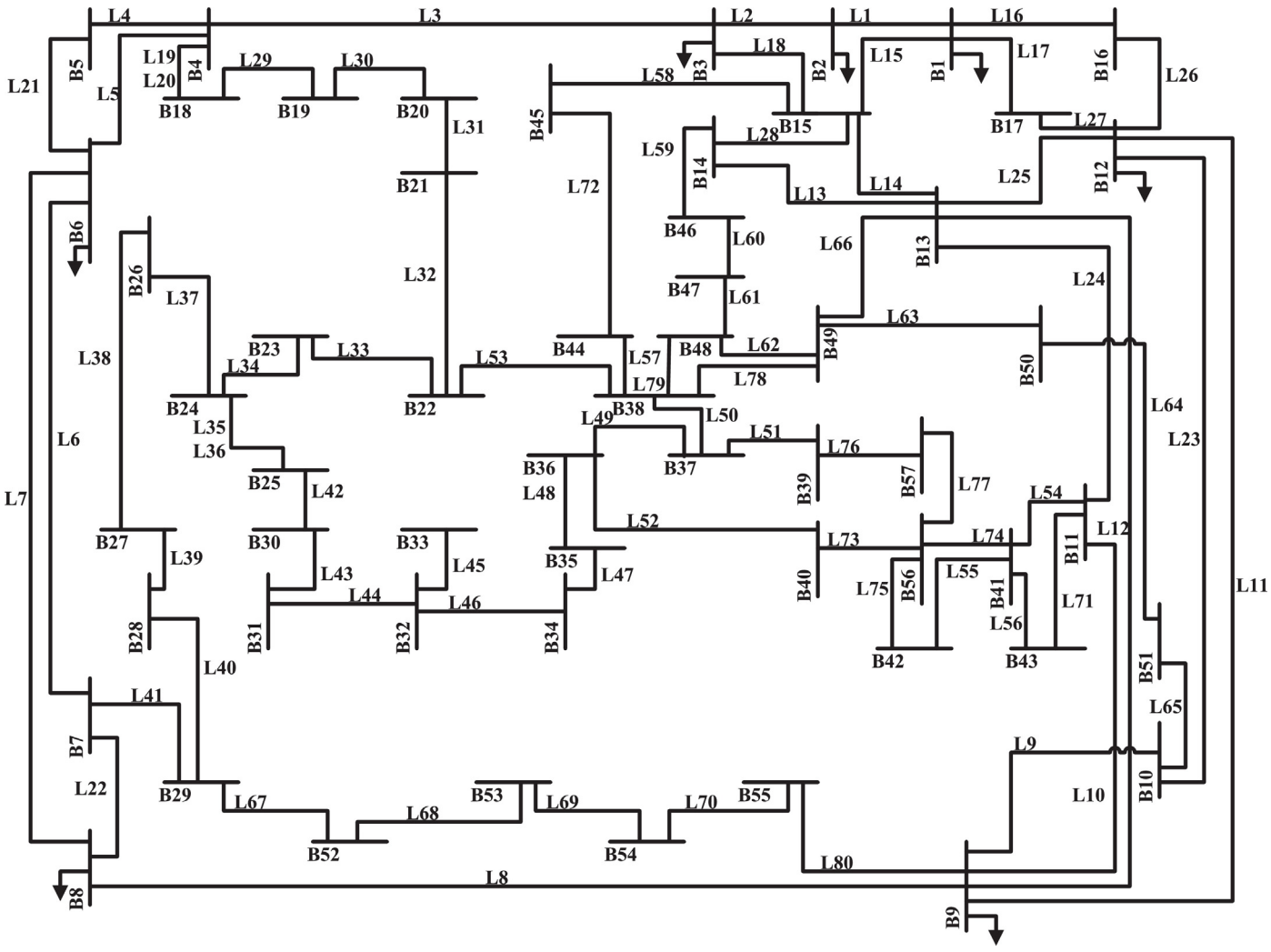

Fig. 4. The IEEE 57-bus test system.

Table 18
Protection decision at $\psi = 0$ MW.

ϵ	(l: protected line, i: protection level)	Total cost
0.001	(4,2),(13,2),(16,2),(17,2),(20,3),(21,3),(23,1) (26,3),(27,3),(29,3),(30,3),(31,2),(32,2),(33,2) (34,3),(35,2),(37,2),(38,2),(39,3),(40,3),(42,3) (43,3),(44,3),(46,3),(47,3),(48,3),(49,1),(51,2) (55,2),(56,2),(57,3),(58,2),(59,3),(60,3),(61,3) (62,1),(63,3),(64,3),(65,3),(67,3),(68,3),(69,3) (70,3),(71,3),(72,2),(75,3),(76,2),(77,3),(80,3)	123
0.01	(4,3),(16,3),(17,3),(19,1),(23,1),(28,1) (29,2),(30,2),(31,2),(32,2),(34,3),(35,1) (37,2),(38,2),(39,2),(40,2),(42,2),(43,2) (44,2),(46,2),(47,2),(48,2),(49,2),(55,3) (56,3),(57,3),(59,2),(60,2),(61,2),(63,2) (64,2),(65,2),(67,2),(68,2),(69,2),(70,2) (77,3),(80,2)	80
0.05	(4,1),(16,1),(17,1),(21,1),(26,1),(27,1) (29,1),(30,1),(31,1),(32,1),(33,1),(34,1) (37,1),(38,1),(39,1),(40,1),(42,1),(43,1) (44,1),(46,1),(47,1),(48,1),(55,1),(56,1) (57,2),(59,1),(60,1),(61,1),(63,1),(64,1) (65,1),(67,1),(68,1),(69,1),(70,1),(71,1) (75,1),(77,2),(80,1)	41
0.10	(4,1),(9,1),(16,1),(17,1),(19,1),(29,1),(30,1) (34,1),(39,1),(40,1),(42,1),(43,1),(44,1) (46,1),(47,1),(48,1),(55,1),(56,1),(57,1) (59,1),(60,1),(61,1),(64,1),(65,1),(67,1) (68,1),(69,1),(70,1),(77,1),(80,1)	30

Table 19
Effect of protection costs on optimal decisions at $\psi = 0$ and $\epsilon = 0.01$.

Cost plan	(l: protected line, i: protection level)
#2	(4,2),(16,2),(17,2),(19,1),(23,1),(26,2),(27,2) (28,1),(29,2),(30,2),(31,2),(32,2),(33,2),(34,2) (35,1),(37,2),(38,2),(39,2),(40,2),(42,2),(43,2) (44,2),(46,2),(47,2),(48,2),(49,1),(55,2),(56,2) (57,3),(59,2),(60,2),(61,2),(62,1),(63,2),(64,2) (65,2),(67,2),(68,2),(69,2),(70,2),(71,2),(75,2) (77,3),(80,2)

as well as more number of transmission lines with enhanced protections.

To study the effect of protection costs in larger systems, we compare the protection decisions under the cost profiles, given in Table 7, and summarized the results in Table 19. The model favors to replace expensive high-reliability protection schemes with more number of the relatively cheaper schemes.

5. Discussion and future research

In this paper, the necessity of the power grid resilience against physical attacks is discussed. However, modern power grids are heavily relied on information and communication technologies that could be maliciously targeted by cyber-attackers to tamper with the grid. Simultaneous cyber-physical attacks could put the

safe and secure operations of the power systems at high risks. To further extend power grid resiliency, it is necessary to develop comprehensive protection models that address cyber and physical attacks together and determine a more inclusive protection plan.

Furthermore, we proposed an effective scenario reduction strategy that significantly reduces the number of scenarios and the computational time accordingly. However, we believe that more research needs to be done to improve the computational efficiency. There are two general approaches to reduce the computational time in this problem, reducing the number of scenarios and parallel computations. The former can be implemented by developing more efficient scenario reduction strategies whereas the latter necessitates reformulating the proposed model such that parallel computing techniques and decomposition methods such as Benders decomposition and scenario decomposition can be utilized.

6. Conclusions

The transmission system security is of the highest priorities of the power system stakeholders. To enhance the resiliency of the transmission system against physical attacks, the MILP optimization model was developed. The model determines the optimal allocation of the enhanced protection schemes to transmission lines. The goal of the model is to minimize the investment costs such that the risk of the load curtailment, caused by a malicious attack, exceeding a certain threshold value be less than the risk tolerance value. Considering the risk in protecting the transmission systems against physical attacks is one of the main contributions of the paper. This contribution provides power system investors with more flexibility comparing to the other models, which protect the system only against worst attack scenarios and are based on the unrealistic assumption that the protected transmission lines can no longer be attacked. The load curtailment is obtained using the modified DC-OPF constraints integrated to our model without considering the generation costs in the objective function. The reason is that the generation cost is not the priority when the power system security is compromised and the supply of power is disrupted temporarily. In fact, any feasible solution that keeps the load curtailment/shedding under the threshold value would be satisfactory in emergency situations. The only obstacle for using the proposed model on a much larger power system is the computer processing time, which is highly depending on the number of attack scenarios. To alleviate the problem, we proposed an effective scenario reduction strategy. The performance of the proposed protection optimization model was tested on the IEEE 6-bus, IEEE 24-bus and IEEE 57-bus test systems. We utilized the scenario reduction strategy and showed the efficacy of the strategy on both reducing the number of scenarios and obtaining the global optimal solutions. The proposed scenario reduction strategy successfully reduced the number of scenarios by 73% and 90% in IEEE 24-bus and IEEE 57-bus test systems, respectively. The experimental results confirmed that conservative protection plans, in which higher risk of unsatisfied demand is not tolerated, necessitate protecting more number of transmission lines as well as utilizing more number of the higher-reliability protection mechanisms, which together increase the investment costs substantially.

Appendix A. Attacks to generators

In this paper, we studied the resiliency of the transmission systems against physical attacks. However, attackers may target generation assets as well to endanger the sources of power generation directly. Our proposed optimization model can be extended to accommodate these attacks too. Eqs. (1), (7) and Eq. (15) need to be modified as follows and Eqs. (23) and (24) be added:

$$Z = \min_{\mathbf{x},\mathbf{y}} \sum_{l=1}^{L}\sum_{i=1}^{I} C_i x_{li} + \sum_{g=1}^{G}\sum_{i=1}^{I} C'_i y_{gi} \tag{20}$$

$$p_g^{\min}(1-\vartheta_{\phi g}) \le p_{\phi g} \le p_g^{\max}(1-\vartheta_{\phi g}) \quad \forall g \in G; \quad \forall \phi \in \Phi \tag{21}$$

$$u_\phi = \sum_{l=1}^{L}\sum_{i=1}^{I} x_{li}\delta_{\phi l}\ln((1-R_i)) + \sum_{g=1}^{G}\sum_{i=1}^{I} y_{gi}\vartheta_{\phi g}\ln((1-R'_i)) \quad \forall \phi \in \Phi \tag{22}$$

$$\sum_{i=1}^{I} y_{gi} = 1 \quad \forall g \in G \tag{23}$$

$$y_{gi} \in \{0,1\} \quad \forall g \in G; \quad \forall i \in I \tag{24}$$

where C'_i is the cost of the generation protection level i; y_{gi} is the binary decision variable which equals 1 if generator g is equipped with protection level i and 0 otherwise; $\vartheta_{\phi g}$ is a binary input parameter which equals to one if the generator g is interdicted in the attack scenario ϕ and 0 otherwise and R'_i is the reliability index of the generator protection type i.

Appendix B. Computational time analysis

All experiments were performed on a 64-bit laptop with an Intel Core i5 2.4 GHz processor and 8 GB RAM. We used IBM ILOG CPLEX Optimization Studio 12.6 as the optimization solver in our experiments. The attack scenarios are obtained using MATLAB R2012a and MatPower [32]. The computation times in MATLAB are trivial.

Table 20 summarizes the computational time for obtaining the optimal protection decisions for the studied test systems. The computation time increases for the larger power systems since the number of potential attack scenarios increase significantly.

Table 20
Computational times.

Test system	Computational time
IEEE 6-bus	3 s
IEEE 24-bus	235 s
IEEE 57-bus	4.2 h

References

[1] G.A. Fenton, N. Sutherland, Reliability-based transmission line design, IEEE Trans. Power Deliv. 26 (2) (2011) 596–606.
[2] Executive office of the President, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages, Tech. Rep., President's Council of Economic Advisers and U.S. Department of Energy's Office of Electricity, Delivery & Energy Reliability with Assistance from the White House Office of Science and Technology, 2013.
[3] Y. Zhu, Y. Jun, T. Yufei, L.S. Yan, H. Haibo, Coordinated attacks against substations and transmission lines in power grids, in: Proceedings of IEEE Global Communications Conference (GLOBCOM), 2014, pp. 655–661.
[4] R. Smith, Assault on California Power Station Raises Alarm on Potential for Terrorism, 2014 http://www.wsj.com/articles/.
[5] S. Tas, M.B. Vicki, Electric Power Vulnerability Models: From Protection to Resilience, Wiley, 2015.
[6] S. Mousavian, J. Valenzuela, J. Wang, Real-time data reassurance in electrical power systems based on artificial neural networks, Electr. Power Systems Res. 96 (2013) 285–295.
[7] J. Salmeron, K. Wood, R. Baldick, Analysis of electric grid security under terrorist threat, IEEE Trans. Power Syst. 19 (2) (2004) 905–912.
[8] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, C. Yang, J. Meza, Severe multiple contingency screening in electric power systems, IEEE Trans. Power Syst. 23 (2) (2008) 406–417.
[9] G. Brown, M. Carlyle, J. Salmeron, K. Wood, Defending critical infrastructure, Interfaces 36 (6) (2006) 530–544.
[10] J.M. Arroyo, Bilevel programming applied to power system vulnerability analysis under multiple contingencies, IET Gen. Transm. Distrib. 4 (2) (2010) 178–190.

[11] J. Salmeron, K. Wood, R. Baldick, Worst-case interdiction analysis of large-scale electric power grids, IEEE Trans. Power Syst. 24 (1) (2009) 96–104.
[12] V.M. Bier, E.R. Gratz, N.J. Haphuriwat, W. Magua, K.R. Wierzbicki, Methodology for identifying near-optimal interdiction strategies for a power transmission system, Reliab. Eng. Syst. Saf. 92 (9) (2007) 1155–1161.
[13] Y. Yao, T. Edmunds, D. Papageorgiou, R. Alvarez, Trilevel optimization in power network defense, IEEE Trans. Syst. Man Cybernet. Part C Appl. Rev. 37 (4) (2007) 712–718.
[14] N. Alguacil, A. Delgadillo, J.M. Arroyo, A trilevel programming approach for electric grid defense planning, Comput. Oper. Res. 41 (2014) 282–290.
[15] A.J. Holmgren, E. Jenelius, J. Westin, Evaluating strategies for defending electric power networks against antagonistic attack, IEEE Trans. Power Syst. 22 (1) (2007) 76–84.
[16] G. Chen, Z.Y. Dong, D.J. Hill, Y.S. Xue, Exploring reliable strategies for defending power systems against targeted attacks, IEEE Trans. Power Syst. 26 (3) (2011) 1000–1009.
[17] P. Cappanera, M.P. Scaparra, Optimal allocation of protective resources in shortest-path networks, Transp. Sci. 45 (1) (2011) 64–80.
[18] C.Y.T. Ma, D.K. Yau, X. Lou, N.S. Rao, Markov game analysis for attack-defense of power networks under possible misinformation, IEEE Trans. Power Syst. 28 (2) (2012) 1676–1686.
[19] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, C. Yang, J. Meza, Identification of severe multiple contingencies in electric power networks, in: Proceedings of the IEEE 37th Annual North American Power Symposium, 2005, pp. 59–66.
[20] A. Pinar, A. Reichert, B. Lesieutre, Computing criticality of lines in power systems, in: IEEE International Symposium on Circuits and Systems, 2007, pp. 65–68.
[21] G.J. Correa, J.M. Yusta, Grid vulnerability analysis based on scale-free graphs versus power flow models, Electr. Power Syst. Res. 101 (2013) 71–79.
[22] A. Delgadillo, J.M. Arroyo, N. Alguacil, Analysis of electric grid interdiction with line switching, IEEE Trans. Power Syst. 25 (2) (2010) 633–641.
[23] J.M. Arroyo, F.J. Fernandez, A genetic algorithm approach for the analysis of electric grid interdiction with line switching, in: Proceedings of 15th IEEE International Conference on Intelligent System Applications to Power Systems, 2009, pp. 1–6.
[24] A. Castillo, Risk analysis and management in power outage and restoration: a literature survey, Electr. Power Syst. Res. 107 (2014) 9–15.
[25] A. dos Santos, M.C. de Barros, P. Correia, Transmission line protection systems with aided communication channels – Part II. Comparative performance analysis, Electr. Power Syst. Res. 127 (2015) 339–346.
[26] Committee on Enhancing the Robustness, Resilience of Future Electrical Transmission, Distribution in the United States to Terrorist Attack, Board on Energy, Environmental Systems, Division on Engineering, Physical Sciences, National Research Council, Terrorism and the Electric Power Delivery System, National Academies Press, 2012.
[27] N. Perera, A.D. Rajapakse, Series-compensated double-circuit transmission-line protection using directions of current transients, IEEE Trans. Power Deliv. 28 (3) (2013) 1566–1575.
[28] Congress of the United States Office of Technology Assessment, Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage, U.S. Government Printing Office, 1990.
[29] F. Shokooh, J.J. Dai, S. Shokooh, J. Tastet, H. Castro, T. Khandelwal, G. Donner, Intelligent load shedding, IEEE Ind. Appl. Mag. 17 (2) (2011) 44–53.
[30] X. Lou, D.K.Y. Yau, H.H. Nguyen, B. Chen, Profit-optimal and stability-aware load curtailment in smart grids, IEEE Trans. Smart Grid 4 (3) (2013) 1411–1420.
[31] A.J. Wood, B.F. Wollenberg, Power Generation, Operation and Control, John Wiley & Sons, 1996.
[32] R.D. Zimmerman, C.E. Murillo-Sanchez, R.J. Thomas, MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education, IEEE Trans. Power Syst. 26 (2011) 12–19.
[33] Subcommittee, IEEE reliability test system, IEEE Trans. Power Apparatus Syst. 98 (1979) 2047–2054.