Leveraging Network Topology Optimization to Strengthen Power Grid Resilience Against Cyber-Physical Attacks

Zhaoxi Liu, *Member, IEEE*, and Lingfeng Wang, *Senior Member, IEEE*

***Abstract*—The contemporary power systems are facing a growing level of risks due to potential deliberate attacks by adversaries. Strengthening the resilience of power grids against malicious cyber-physical attacks is emerging as a critical task considering the importance of power systems to the entire society. In this article, a bilevel optimization model is developed to formulate the coordinated cyber-physical attacks against the power grids. In order to enhance the resilience of the power systems, a networked topology optimization (NTO) based model is proposed to mitigate the coordinated cyber-physical attacks. Resilience metrics are proposed to evaluate the power system resilience against the coordinated cyber-physical attacks. Case studies were conducted on the modified IEEE 57-bus and 118-bus systems to illustrate the impacts of coordinated cyber-physical attacks as well as validate the proposed NTO based approach. The results of the case studies show that the proposed NTO based mitigation strategy can effectively reduce the load loss of the power system under the coordinated cyber-physical attacks. The resilience of the system is improved by the proposed NTO based approach compared with the conventional optimal redispatch (OR) and optimal transmission switching (OTS) based remedial methods.**

***Index Terms*—Cyber-physical attacks, cybersecurity, network topology optimization (NTO), power grid security, power system resilience.**

NOMENCLATURE

Indices and Sets

b	Index of bays in substations with breaker-and-a-half configuration.
g	Index of generation units.
i, j	Index of buses (substations) in the grid.
t/τ	Index of time.
$\mathcal{B}_i$	Set of bays in substation i with breaker-and-a-half configuration.
$\mathcal{E}$	Set of transmission branches in the grid.
$\mathcal{G}/\mathcal{G}_i$	Set of generation units in the grid/connected to bus i.
$\mathcal{N}$	Set of buses (substations) in the grid.
$\mathcal{N}_\varsigma/\mathcal{N}_\nu$	Set of buses (substations) with/without bus-splitting (BS) possibility in the grid.
$\mathcal{T}$	Set of time intervals in the system restoration process after attack.

Parameters

M	A large-enough positive number.
N^{BS}	Maximum number of BS actions in the grid.
N^{TS}	Maximum number of transmission-switching (TS) actions in the grid.
N^{NTO}	Maximum number of overall BS and TS actions.
p_g^{max}	Active power output limit of generation unit g.
$p_{i,j}^{\mathsf{max}}$	Power transmission limit of the transmission branch between bus i and bus j.
$p_{i,t}$	Demand at bus i at time t.
$s_{g,t}$	Status indicator of generation unit g at time t.
$s_{i,j,t}$	Status indicator of the transmission branch between bus i and bus j at time t.
$x_{i,j}$	Reactance of the transmission branch between bus i and bus j.
Λ^{CG}	Maximum number of generation units compromised by cyberattacks.
Λ^{CS}	Maximum number of substations compromised by cyberattacks.
Λ^{P}	Maximum number of transmission branches compromised by physical attacks.
τ^{CG}	Restoration time of generation units to recover from cyberattacks.
τ^{CS}	Restoration time of substations to recover from cyberattacks.
τ^{P}	Restoration time of transmission branches to recover from physical attacks.

Variables

$p_{g,t}$	Active power output of generation unit g at time t.
$p_{g,t}^{\mathsf{I}}/p_{g,t}^{\mathsf{II}}$	Active power output of generation unit g if it is connected to busbar I/II by BS action at time t.
$p_{i,t}^{\mathsf{I}}/p_{i,t}^{\mathsf{II}}$	Demand connected to busbar I/II by BS action at bus (substation) i at time t.
$p_{i,j,t}$	Active power on the transmission branch between bus i and bus j at time t.
$w_{g,t}$	Connection decision of generation unit g in BS action at time t.
$w_{i,t}^{\mathsf{D}}$	Connection decision of demand at bus (substation) i in BS action at time t.

Manuscript received March 23, 2020; revised August 11, 2020; accepted September 12, 2020. Date of publication October 1, 2020; date of current version February 26, 2021. This work was supported in part by the U.S. National Science Foundation under Award ECCS1711617. Paper no. TSG-00423-2020. *(Corresponding author: Lingfeng Wang.)*

The authors are with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211 USA (e-mail: zhaoxil@uwm.edu; l.f.wang@ieee.org).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2020.3028123

$w^{\mathsf{Fr}}_{i,j,t}$ Connection decision of the transmission branch between bus i and bus j in BS action at bus (substation) i at time t.

$w^{\mathsf{To}}_{i,j,t}$ Connection decision of the transmission branch between bus i and bus j in BS action at bus (substation) j at time t.

$w^{\mathsf{I}}_{i,b,t}$ Connection decision of the circuit closer to busbar I in bay b at bus (substation) i with breaker-and-a-half configuration at time t.

$w^{\mathsf{II}}_{i,b,t}$ Connection decision of the circuit closer to busbar II in bay b at bus (substation) i with breaker-and-a-half configuration at time t.

$z_{i,t}$ Bus-splitting decision of bus i at time t.

$z_{i,j,t}$ Transmission-switching decision of the transmission branch between bus i and bus j at time t.

α_g Cyberattack action on generation unit g.

α_i Cyberattack action on bus (substation) i.

$\alpha_{i,j}$ Physical attack action on the transmission branch between bus i and bus j at time t.

$\delta_{i,t}$ Curtailed demand at bus i at time t.

$\delta^{\mathsf{I}}_{i,t}/\delta^{\mathsf{II}}_{i,t}$ Curtailed demand at busbar I/II of bus (substation) i at time t.

$\vartheta_{i,t}$ Voltage phase angle at bus i at time t.

$\vartheta^{\mathsf{I}}_{i,t}/\vartheta^{\mathsf{II}}_{i,t}$ Voltage phase angle at busbar I/II of bus (substation) i at time t.

$\vartheta^{\mathsf{Fr}}_{i,j,t}$ Voltage phase angle at the busbar in substation i connected to the transmission branch between bus i and bus j at time t.

$\vartheta^{\mathsf{To}}_{i,j,t}$ Voltage phase angle at the busbar in substation j connected to the transmission branch between bus i and bus j at time t.

Functions

$f(\tau, t)$ Step function of the system component status.

I. Introduction

As ONE of the critical infrastructures in the modern society, the power systems are responsible for a reliable, secure and resilient supply of electricity to billions of customers around the world. Disturbances to the normal operation of power systems can cause far reaching impacts on nearly every industry, and have enormous financial and security effects to the entire society. In recent years, the power systems are facing growing risks of extreme events from not only the natural disasters but also the malicious attacks by adversaries [1]. A real-world example is the successive deliberate attacks on the Ukrainian power system in 2015 and 2016 in which large-scale power supply interruptions were caused [2]. Ensuring the security of the power system operation is emerging as an urgent task for both academia and industry.

Strengthening the resilience of the power systems is critical to effectively and efficiently reduce the risks to the reliability and security of the grids in the face of uncertainties [3]. Recent efforts have been actively devoted to the research on the power system resilience under extreme events. The fundamental concepts, metrics and quantification of the power system resilience are introduced in [4], [5], and a resilience assessment framework is proposed. To enhance the power system resilience against the natural disasters, an integrated preventive and emergency response framework is proposed in [6]. Meanwhile, a sequential proactive operational strategy is proposed in [7] to enhance the system resilience under an unfolding extreme weather-related event. In [8], a robust optimization model is proposed for the integrated planning of electricity and natural gas transportation systems to enhance the power grid resilience. Further, strategic islanding of the power systems has also been investigated and proposed to boost the system resilience under extreme weather events [9], [10].

Recently, a few studies have been performed focusing on the impacts of cyber-physical attacks on the power system reliability and security. In [11], the authors propose to detect the line failures after the cyber-physical attacks on the power grid by using Bayesian regression. An attack-resilient cyber-physical security framework is proposed in [12] for the wide-area monitoring, protection and control (WAMPAC) applications in power systems. A defense-in-depth architecture covering both the infrastructure and application layers is introduced and discussed in detail in this article. Meanwhile, the works in [13]–[15] investigate the consequences of the cyber-physical attacks in which the attackers inject false information to the state and topology data for the state estimation of the power system to mask the physical attack on the grid, and propose the countermeasures against the attacks. In [16], the cyber-physical switching attacks are modeled with a coordinated switching sequence to a circuit breaker (CB) in the smart grid to disrupt the system operation. In order to overcome the data limitations for the resilience analytics of cyber-physical attacks on the distribution network, [17] proposes a vulnerability assessment by applying the stochastic counterfactual risk analysis. A reliability evaluation framework based on the cyber-physical model of the active distribution system is proposed in [18]. In [19], the Ex-ante and Ex-post attacks on the real-time pricing schemes of the power market are investigated. The sequential attack which may enlarge the blackout size in the grid is studied in [20] and its impacts on the resilience of the power system is evaluated. The game theory is used in [21], [22] to identify the optimal security resource allocation in power systems against antagonistic attacks, and the power system reliability is evaluated.

In order to enhance the power system resilience, the work in this article focuses on the remedial strategies of the system operator to mitigate the impacts of the cyber-physical attacks launched on the grid to knock out the critical components including generation units, substations and transmission lines deliberately. The network topology optimization (NTO) can increase the flexibility of the power system reconfiguration by performing not only the transmission switching on the branches but also the bus splitting within the substation configuration. In [23], an NTO model is proposed to relieve the transmission system congestion. The NTO technology is also considered in [24] to evaluate the power system reliability with dynamic thermal rating (DTR). An NTO based day-ahead scheduling model is proposed in [25] for a cost-effective solution of the network-constrained unit commitment problem. The

existing studies have shown that NTO can boost the flexibility of the system operations. Thus, in this study, the NTO technique is employed to mitigate the impacts of the coordinated cyber-physical attacks on power systems.

In the existing researches, the optimal redispatch (OR) is generally considered as the response of the system operator against the cyber and physical attacks on the grid. However, as discussed above, the system resilience under the attacks can be improved by considering the reconfiguration of the network topology. Thus, in this article, the NTO technique is applied in response to the cyber-physical attacks to enhance the system resilience by considering both the transmission-switching and bus-splitting possibilities. Meanwhile, the coordinated cyber-physical attack model is analyzed in this article which maximizes the potential outcome of the coordinated attack actions with consideration of the restoration process of the grid in the bilevel model, which has not been covered in the existing literature. Further, in the existing NTO models in literature, the generalized two-bus model of the substation is applied. However, the generalized two-bus model may result in infeasible solutions when the bus configuration in the substation is the breaker-and-a-half configuration which is widely used in power systems. Therefore, in this article, the detailed bus configurations of the substations are considered in the proposed NTO model to prevent infeasible solutions for the breaker-and-a-half configuration and over-optimistic results. The major contributions of this article are summarized as follows:

- A bilevel optimization model is proposed to model the coordinated cyber-physical attacks against the power grid. The optimal attack actions on the generation units, substations and transmission branches are determined accordingly to maximize the total load curtailment of the grid considering the system restoration processes and the reactive operations by the system operator.
- A detailed NTO based model is developed to minimize the load losses in the grid against the coordinated cyber-physical attacks. Compared with the conventional optimal power flow based redispatch (OR) and the optimal transmission switching (OTS) strategies, the NTO model can further explore the flexibility of the system operations and better mitigate the impacts of the attacks.
- Metrics are proposed to evaluate the power system resilience against the coordinated cyber-physical attacks. Accordingly, the resilience of the grid under attacks with different system operation strategies is assessed and compared.

The rest of this article is organized as follows. The general idea of the NTO operation is introduced in Section II. In Section III, a bilevel optimization model of the coordinated cyber-physical attacks against the power systems is proposed. Then, a detailed NTO based model for the power system operations against the coordinated cyber-physical attacks is developed in Section IV. The resilience metrics of the power systems under the coordinated cyber-physical attacks are proposed in Section V. In Section VI, the results of the case studies on the proposed NTO model for the system operations against the coordinated cyber-physical attacks are presented. The results, findings and main achievements of the proposed model are discussed in Section VII, followed by the conclusions in Section VIII.

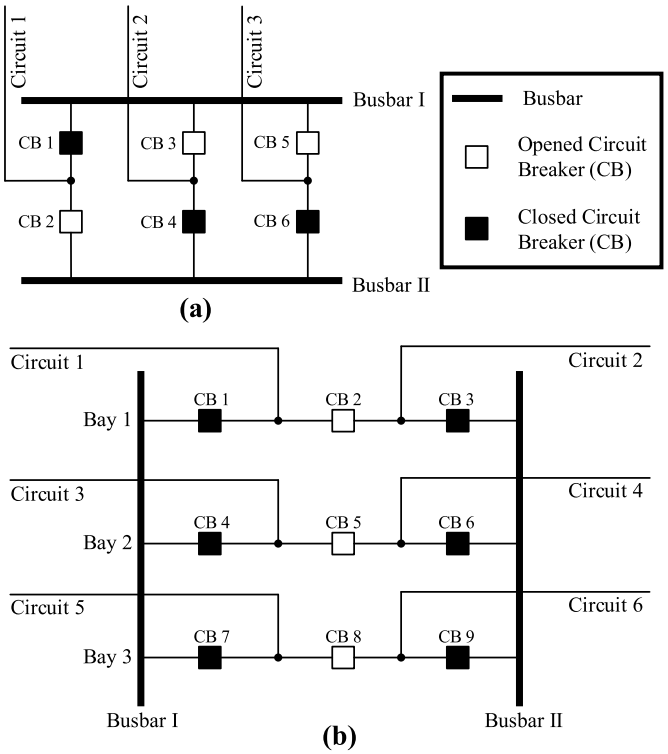


Fig. 1. Bus-Splitting Actions in Substations with (a) Double-bus Configuration and (b) Breaker-and-a-half Configuration.

II. Network Topology Optimization for Power System Reconfiguration

In the power system reconfiguration researches, the optimal transmission switching (OTS) is conventionally used to modify the topology of the grid strategically. The switching of the transmission branches in the grid is considered as a controllable variable in OTS. In order to further increase the flexibility of the power system reconfiguration, the Network Topology Optimization (NTO) approach considers not only the transmission-switching (TS) actions but also the bus-splitting (BS) actions in the analysis [23]. The generic idea of NTO is introduced below.

In the transmission systems, the bus configurations with two busbars (e.g., double-bus configuration and breaker-and-a-half configuration) are widely deployed in substations for high flexibility and reliability [26]. With such bus configurations consisting of two busbars in the substations, it is possible to further reconfigure the arrangement within the substations by performing the BS actions. In normal operations, the circuit breakers (CBs) in such configurations are all closed, and the two busbars in the substation are regarded as one node (bus) in the node-branch model for the power system analysis. However, as shown in Fig. 1, the two busbars in the double-bus and breaker-and-a-half configurations can be separated into two individual buses by opening at least one CB connected to each circuit (for the double-bus configuration) or in each bay (for the breaker-and-a-half configuration) in the

substation. As a result, the two busbars can be separated and act as two individual nodes (buses) in the analysis with the BS actions.

Accordingly, with the BS actions, the topology of the power system can be reconfigured down to the substation arrangement level, and a higher degree of freedom is enabled for the system reconfiguration when needed. A generalized reconfiguration model of the substations with the two-busbar configurations as shown in Fig. 2 is used to demonstrate the TS and BS actions in NTO. In a substation with two busbars, the two busbars can be either connected (as a bus) or separated (as two independent buses). When the two busbars are separated, they act as two independent nodes in the node-branch model of the power system. The transmission branches (as well as the generation units and load feeders) connected to the substation can be connected to either busbar based on the decision of the system operator. Further, the transmission branches can be switched off according to the TS actions in the system operations.

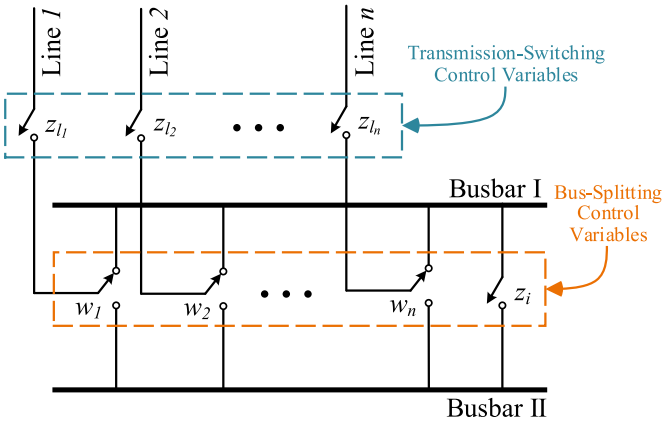


Fig. 2. Generalized Model of Transmission-Switching and Bus-Splitting Actions in NTO.

III. Bilevel Model of Coordinated Cyber-Physical Attacks

In this study, the proposed model focuses on the coordinated cyber-physical attacks on the grid to damage the normal operation of the power system by disconnecting or tripping the substations, generation units and transmission branches directly. It is assumed that the attackers aim to maximize the damage to the grid by coordinating the cyber attacks and physical attacks. The physical attacks are assumed to be performed on the transmission branches while the cyberattacks are assumed to be performed on the generation units and substations in the grid. In practice, the cyberattacks on the substations and generation units can be mounted by intruding the supervisory control and data acquisition (SCADA) systems of the substations and power plants (e.g., the successful cyberattack on the Ukrainian power grid in 2015), and forcing the disconnection of the substations and generation units from the grid via false comments [22], [27], [28]. The intrusion can be achieved by exploiting the vulnerabilities not only in the SCADA systems but also in the software and operation systems that are connected to the SCADA networks (or station LANs) with malware [22], [27]–[29]. The down time of the substations and generation units will last until the attacks are cleared or isolated from the control systems. The physical attacks on the transmission lines can be mounted through physical sabotage including shooting the isolators, sawing off the shackles that hold up the power lines, and damaging the transmission towers, etc., which have been reported in real-world incidents [30]. The transmission lines will be opened by protection or control systems until the physical damage is repaired. Therefore, in the proposed model, a transmission branch is assumed to be switched off the network if it is hit by the physical attacks. It is assumed that all the breakers in a substation are forced to be switched off when the substation is compromised by the cyberattacks. Meanwhile, a generation unit is assumed to be tripped when it is compromised by the cyberattacks. When the cyber and physical attacks are triggered by the adversaries, the affected components in the grid including the generation units, substations and transmission branches remain out-of-service until they are restored, and different restoration times will be needed to clear the cyber and physical attacks. The categories of potential cyberattacks on power systems are broad. The proposed attack model in this article does not aim to cover various types of cyberattacks but focuses on the most direct and immediate cyberattacks on the grid. Thus, for the cyberattacks on the substations in this article, the proposed model mainly considers the malicious actions to damage the normal operation of the grid by disconnecting the substations through tripping the circuit breakers directly. Such cyberattack has been proved to be feasible in reality and can lead to serious damage to the grid by the example of the cyberattack on the Ukrainian power grid in 2015 [27], [28]. Other types of cyberattacks (e.g., false data injection (FDI) attacks and cyberattacks on the transformers) are not covered by the attack model in this article.

Generally, the system operator will perform the optimal power flow based redispatch to minimize the load curtailment according to the statuses of components in the grid during the restoration processes after the attacks are triggered. The objective of the attacks is to maximize the total load curtailment considering the system restoration and the optimal redispatch decisions of the system operator. Therefore, the attacks can be formulated with a bilevel model. The bilevel model of the coordinated cyber-physical attacks on the grid is illustrated in Fig. 3. In the bilevel model, the attacker considers the potential response of the system operator with the optimal dispatch strategies to the attack vector. As shown in Fig. 3, the lower level model formulates the optimal dispatch strategies of the system operator under the attack actions determined by the upper level model, and generates the expected consequence of both the attack actions and the optimal dispatch strategies on the grid. The expected consequence is fed back to the upper level model to evaluate and optimize the outcome of the attack vector. Thus, the solution of the bilevel model provides the optimal attack decisions considering the reaction of the system operator.

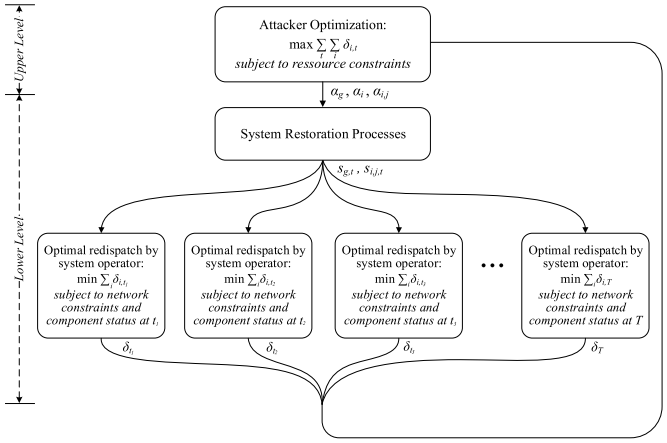


Fig. 3. Bilevel Model of Coordinated Cyber-Physical Attacks on Power Systems.

The detailed formulation of the coordinated cyber-physical attack model is presented as follows.

$$\max_{\alpha_g,\alpha_i,\alpha_{i,j}} \sum_{t\in\mathcal{T}}\sum_{i\in\mathcal{N}} \delta^*_{i,t} \tag{1}$$

Subject to

$$\sum_{g\in\mathcal{G}} \alpha_g \le \Lambda^{\mathsf{CG}} \tag{2}$$

$$\sum_{i\in\mathcal{N}} \alpha_i \le \Lambda^{\mathsf{CS}} \tag{3}$$

$$\sum_{(i,j)\in\mathcal{E}} \alpha_{i,j} \le \Lambda^{\mathsf{P}} \tag{4}$$

$$s_{g,t} = \sup\left\{\alpha_g f\left(\tau^{\mathsf{CG}},t\right), \alpha_i f\left(\tau^{\mathsf{CS}},t\right)\right\} \quad \forall g\in\mathcal{G}_i \quad \forall i\in\mathcal{N} \tag{5}$$

$$s_{i,j,t} = \sup\left\{\alpha_{i,j} f\left(\tau^{\mathsf{P}},t\right), \alpha_i f\left(\tau^{\mathsf{CS}},t\right), \alpha_j f\left(\tau^{\mathsf{CS}},t\right)\right\} \quad \forall (i,j)\in\mathcal{E} \tag{6}$$

where α_g and α_i are the cyber attack action decisions against the generation units and substations respectively, and $\alpha_{i,j}$ are the physical attack decisions against the transmission branches. They equal 1 if the corresponding component is targeted. Otherwise, they equal 0. $s_{g,t}$ and $s_{i,j,t}$ are the status indicators of the generation units and transmission branches at time t respectively. They equal 1 when the corresponding generation unit or transmission branch is out-of-service. Otherwise, they equal 0. $f(\tau,t)$ is a step function of t with parameter τ as defined below.

$$f(\tau,t) = \begin{cases} 1, & \text{if } t\le\tau \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

Considering the statuses of components in the grid due to the attacks, the optimal redispatch problem of the system operator is presented as follows.

$$\delta^*_{i,t} = \arg\min \sum_{i\in\mathcal{N}} \delta_{i,t} \tag{8}$$

Subject to

$$-Ms_{i,j,t} \le \frac{\vartheta_{i,t}-\vartheta_{j,t}}{x_{i,j}} - p_{i,j,t} \le Ms_{i,j,t},\ \forall (i,j)\in\mathcal{E} \tag{9}$$

$$\sum_{g\in\mathcal{G}_i} p_{g,t} - \left(p_{i,t}-\delta_{i,t}\right) - \sum_{j\in\mathcal{N}:(i,j)\in\mathcal{E}} p_{i,j,t} = 0,\ \forall i\in\mathcal{N} \tag{10}$$

$$-p^{\mathsf{max}}_{i,j}\left(1-s_{i,j,t}\right) \le p_{i,j,t} \le p^{\mathsf{max}}_{i,j}\left(1-s_{i,j,t}\right),\ \forall (i,j)\in\mathcal{E} \tag{11}$$

$$0 \le p_{g,t} \le p^{\mathsf{max}}_{g}\left(1-s_{g,t}\right),\ \forall g\in\mathcal{G} \tag{12}$$

$$0 \le \delta_{i,t} \le p_{i,t},\ \forall i\in\mathcal{N} \tag{13}$$

The objective of the system operator is to minimize the load curtailment in the grid as (8) considering the generation unit status $s_{g,t}$ and transmission branch status $s_{i,j,t}$. Constraints (9)–(10) formulate the power flows in the grid, and constraints (11)–(12) are the active power transmission limits of the transmission branches and the output limits of the generation units, respectively. Equation (13) is the constraint of the load curtailment which is limited by the demand at the bus.

IV. NTO Based Strategies Against Coordinated Cyber-Physical Attacks

In order to further mitigate the impacts of the coordinated cyber-physical attacks, an NTO based model is proposed for the system operator by increasing the flexibility of the system reconfiguration with both transmission-switching and bus-splitting actions. At time t in the system restoration processes, the optimization problem for the system operator based on NTO with the statuses of system components can be presented as follows.

The objective of the system operator is to minimize the total load curtailment in the grid as (14). The first term in (14) is the load curtailment at the buses without BS actions and the second term is the curtailed load connected to busbars I and II at the buses with BS actions.

$$\min \sum_{i\in\mathcal{N}_v} \delta_{i,t} + \sum_{i\in\mathcal{N}_\varsigma} \left(\delta^{\mathsf{I}}_{i,t} + \delta^{\mathsf{II}}_{i,t}\right) \tag{14}$$

The operation of the NTO is subject to the network constraints. Constraints (15)–(18) are the power flow model based on the statuses of the transmission branches in the restoration processes after the attacks and the TS decision at the moment, where $z_{i,j,t}$ is the TS decision of the transmission branch between bus i and bus j at time t. It equals 1 if the transmission branch is switched off. Otherwise, it equals 0.

$$-M\left(s_{i,j,t}+z_{i,j,t}\right) \le \frac{\vartheta^{\mathsf{Fr}}_{i,j,t}-\vartheta^{\mathsf{To}}_{i,j,t}}{x_{i,j}} - p_{i,j,t},\quad \forall i\in\mathcal{N},(i,j)\in\mathcal{E} \tag{15}$$

$$\frac{\vartheta^{\mathsf{Fr}}_{i,j,t}-\vartheta^{\mathsf{To}}_{i,j,t}}{x_{i,j}} - p_{i,j,t} \le M\left(s_{i,j,t}+z_{i,j,t}\right),\ \forall i\in\mathcal{N},(i,j)\in\mathcal{E} \tag{16}$$

$$-p^{\mathsf{max}}_{i,j}\left(1-s_{i,j,t}\right) \le p_{i,j,t} \le p^{\mathsf{max}}_{i,j}\left(1-s_{i,j,t}\right),\ \forall (i,j)\in\mathcal{E} \tag{17}$$

$$-p^{\mathsf{max}}_{i,j}\left(1-z_{i,j,t}\right) \le p_{i,j,t} \le p^{\mathsf{max}}_{i,j}\left(1-z_{i,j,t}\right),\ \forall (i,j)\in\mathcal{E} \tag{18}$$

Constraints (19)–(24) ensure that the voltage phase angle on either end of the transmission branch is consistent with the bus or busbar it is connected to. $w^{\mathsf{Fr}}_{i,j,t}$ and $w^{\mathsf{To}}_{i,j,t}$ indicate the busbars that the transmission branch is connected to. When $w^{\mathsf{Fr}}_{i,j,t}$ and/or $w^{\mathsf{To}}_{i,j,t} = 0$, it means the transmission branch is connected to busbar I at substation i and/or j in the BS action respectively. When $w^{\mathsf{Fr}}_{i,j,t}$ and/or $w^{\mathsf{To}}_{i,j,t} = 1$, it means the transmission branch is connected to busbar II.

$$\vartheta^{\mathsf{Fr}}_{i,j,t} = \vartheta_{i,t},\ 8i \in \mathcal{N}_v, (i,j) \in \mathcal{E} \tag{19}$$

$$\vartheta^{\mathsf{To}}_{i,j,t} = \vartheta_{j,t},\ 8j \in \mathcal{N}_v, (i,j) \in \mathcal{E} \tag{20}$$

$$-Mw^{\mathsf{Fr}}_{i,j,t} \le \vartheta^{\mathsf{Fr}}_{i,j,t} - \vartheta^{\mathsf{I}}_{i,t} \le Mw^{\mathsf{Fr}}_{i,j,t},\ 8i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{21}$$

$$-M\left(1 - w^{\mathsf{Fr}}_{i,j,t}\right) \le \vartheta^{\mathsf{Fr}}_{i,j,t} - \vartheta^{\mathsf{II}}_{i,t} \le M\left(1 - w^{\mathsf{Fr}}_{i,j,t}\right), \quad \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{22}$$

$$-Mw^{\mathsf{To}}_{i,j,t} \le \vartheta^{\mathsf{To}}_{i,j,t} - \vartheta^{\mathsf{I}}_{j,t} \le Mw^{\mathsf{To}}_{i,j,t},\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{23}$$

$$-M\left(1 - w^{\mathsf{To}}_{i,j,t}\right) \le \vartheta^{\mathsf{To}}_{i,j,t} - \vartheta^{\mathsf{II}}_{j,t} \le M\left(1 - w^{\mathsf{To}}_{i,j,t}\right), \quad \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{24}$$

Constraint (25) keeps the power balance at the buses without BS actions, while constraints (26)–(27) model the power balance at busbars I and II of the buses with BS actions in the grid.

$$\sum_{g \in \mathcal{G}_i} p_{g,t} - \left(p_{i,t} - \delta_{i,t}\right) - \sum_{j \in \mathcal{N}:(i,j) \in \mathcal{E}} p_{i,j,t} = 0,\ \forall i \in \mathcal{N}_v \tag{25}$$

$$\sum_{g \in \mathcal{G}_i} p^{\mathsf{I}}_{g,t} - \left(p^{\mathsf{I}}_{i,t} - \delta^{\mathsf{I}}_{i,t}\right) - \sum_{j \in \mathcal{N}:(i,j) \in \mathcal{E}} p^{\mathsf{I}}_{i,j,t} = 0,\ i \in \mathcal{N}_\varsigma \tag{26}$$

$$\sum_{g \in \mathcal{G}_i} p^{\mathsf{II}}_{g,t} - \left(p^{\mathsf{II}}_{i,t} - \delta^{\mathsf{II}}_{i,t}\right) - \sum_{j \in \mathcal{N}:(i,j) \in \mathcal{E}} p^{\mathsf{II}}_{i,j,t} = 0,\ \forall i \in \mathcal{N}_\varsigma \tag{27}$$

Constraints (28)–(32) are the load shedding constraints considering the BS actions, where $w^{\mathsf{D}}_{i,t}$ indicates the busbar that the load is connected to if a BS action is performed at bus i. When $w^{\mathsf{D}}_{i,t} = 0$, it means the load is connected to busbar I. When $w^{\mathsf{D}}_{i,t} = 1$, it means the load is connected to busbar II.

$$0 \le \delta_{i,t} \le p_{i,t},\ \forall i \in \mathcal{N}_v \tag{28}$$

$$0 \le \delta^{\mathsf{I}}_{i,t} \le p^{\mathsf{I}}_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{29}$$

$$0 \le \delta^{\mathsf{II}}_{i,t} \le p^{\mathsf{II}}_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{30}$$

$$p^{\mathsf{I}}_{i,t} = p_{i,t}\left(1 - w^{\mathsf{D}}_{i,t}\right),\ \forall i \in \mathcal{N}_\varsigma \tag{31}$$

$$p^{\mathsf{II}}_{i,t} = p_{i,t}w^{\mathsf{D}}_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{32}$$

Constraints (33)–(34) are the output constraints of the generation units considering the BS actions, where $w_{g,t}$ indicates the busbar that generation unit g is connected to in the BS action. When $w_{g,t} = 0$, it means generation unit g is connected to busbar I. When $w_{g,t} = 1$, it means generation unit g is connected to busbar II.

$$0 \le p^{\mathsf{I}}_{g,t} \le p^{\mathsf{max}}_g\left(1 - w_{g,t}\right),\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{33}$$

$$0 \le p^{\mathsf{II}}_{g,t} \le p^{\mathsf{max}}_g w_{g,t},\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{34}$$

Constraints (35)–(40) ensure that the power flow on the transmission branch is consistent with the power flow from/to the busbar it is connected to if there is a BS action. Constraint (41) means the voltage phase angles of the two busbars in a substation must be identical if there is no BS action in the substation, where $z_{i,t}$ indicates the BS action at bus i. When $z_{i,t} = 1$, it means there is a BS action at bus i. Otherwise $z_{i,t} = 0$.

$$-\left(1 - w^{\mathsf{Fr}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j} \le p^{\mathsf{I}}_{i,j,t} \le \left(1 - w^{\mathsf{Fr}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j}, \quad \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{35}$$

$$-w^{\mathsf{Fr}}_{i,j,t}p^{\mathsf{max}}_{i,j} \le p^{\mathsf{II}}_{i,j,t} \le w^{\mathsf{Fr}}_{i,j,t}p^{\mathsf{max}}_{i,j},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{36}$$

$$-\left(1 - w^{\mathsf{To}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j} \le p^{\mathsf{I}}_{j,i,t} \le \left(1 - w^{\mathsf{To}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j}, \quad \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{37}$$

$$-w^{\mathsf{To}}_{i,j,t}p^{\mathsf{max}}_{i,j} \le p^{\mathsf{II}}_{j,i,t} \le w^{\mathsf{To}}_{i,j,t}p^{\mathsf{max}}_{i,j},\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{38}$$

$$p_{i,j,t} = p^{\mathsf{I}}_{i,j,t} + p^{\mathsf{II}}_{i,j,t},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{39}$$

$$p_{i,j,t} = -\left(p^{\mathsf{I}}_{j,i,t} + p^{\mathsf{II}}_{j,i,t}\right),\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{40}$$

$$-Mz_{i,t} \le \vartheta^{\mathsf{I}}_{i,t} - \vartheta^{\mathsf{II}}_{i,t} \le Mz_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{41}$$

The model based on the general bus-splitting idea of NTO can be applied freely for the well known double-bus configuration of the substation bus scheme. However, for the breaker-and-a-half configuration, which is widely employed globally due to high flexibility and reliability while being more economical compared with the double-bus configuration, the bus-splitting action strategies need to be constrained as certain strategies of the bus-splitting actions may not be feasible according to the specific arrangement of the configuration. Fig. 4 demonstrates an example of the breaker-and-a-half configuration in the substation. For instance, a bus-splitting strategy with Circuits 1, 2, 3, 5 connected to busbar I and Circuits 4, 6 connected to busbar II is a valid solution by closing CB 1, 2, 4, 6, 7, 9 while opening CB 3, 5, 8 in the substation. However, a bus-splitting strategy with Circuits 1, 3, 6 connected to one busbar and Circuits 2, 4, 5 connected to another busbar is infeasible in practice for the arrangement shown in Fig. 4.

In order to prevent the infeasible solutions for the breaker-and-a-half configuration, the following action constraint is imposed for the circuits in each bay of the breaker-and-a-half configuration.

$$w^{\mathsf{I}}_{i,b,t} \le w^{\mathsf{II}}_{i,b,t},\ \forall b \in \mathcal{B}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{42}$$

where $w^{\mathsf{I}}_{i,b,t}$ and $w^{\mathsf{II}}_{i,b,t}$ are the connection decisions of the circuits closer to busbar I and II respectively in bay b at bus (substation) i with breaker-and-a-half configuration at time t. Constraint (42) ensures that a circuit can only be connected to the busbar at the far-end when the other circuit in the same bay is also connected to that busbar. The full formulation of the optimization problem for the proposed NTO model is presented in the Appendix of this article.

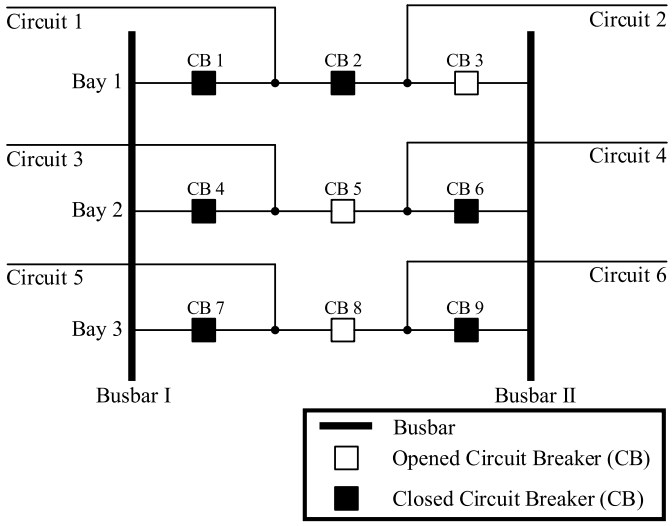


Fig. 4. Illustration of the Breaker-and-a-half Configuration in Substations.

V. Power System Resilience Enhancement Evaluation

In order to assess the performance of the power system operations in boosting the resilience of the grid against the malicious cyber-physical attacks, the power system resilience level should be evaluated quantitatively. The system resilience in engineering is generally evaluated based on the resilience triangle and more recently the multi-phase resilience trapezoid [5]. The concept of the resilience trapezoid is proposed in [4], [5] (similar concepts have also been provided in other works, e.g., [31]) to describe the resilience of the system. It depicts all the phrases of the system during an event and the transition between the states. The resilience trapezoid shows how low the resilience indicator of the system may drop during the event and the restoration process, and how fast it can recover to the pre-event state under the restoration and operation of the system. The shape and area of the resilience trapezoid can provide complementary and quantitative information on the resilience performance of the system in the event. Based on the concepts of the resilience trapezoid and percentage of service provided in measuring the resilience of energy systems [32], resilience indicators R_t and $R_{\%}$ are defined as follows to assess the resilience level of the power systems under the coordinated cyber-physical attacks in this study.

$$R_t = \frac{P_t^{\mathsf{S}}}{P_t} = \frac{\sum_{i\in\mathcal{N}} p_{i,t}^{\mathsf{S}}}{\sum_{i\in\mathcal{N}} p_{i,t}} = \frac{\sum_{i\in\mathcal{N}} \left(p_{i,t} - \delta_{i,t}\right)}{\sum_{i\in\mathcal{N}} p_{i,t}} \tag{43}$$

$$R_{\%} = \frac{\sum_{t\in\mathcal{T}} P_t^{\mathsf{S}}}{\sum_{t\in\mathcal{T}} P_t} = \frac{\sum_{t\in\mathcal{T}} \sum_{i\in\mathcal{N}} \left(p_{i,t} - \delta_{i,t}\right)}{\sum_{t\in\mathcal{T}} \sum_{i\in\mathcal{N}} p_{i,t}} \tag{44}$$

where P_t is the original electricity supplied to the customers by the power system without attacks, P_t^{S} is the total electricity actually supplied, and $p_{i,t}^{\mathsf{S}}$ is the actual electricity supplied at bus i at time t.

The total electricity actually supplied to the customers in the power system under the attacks will never exceed the original electricity supplied to the customers without attacks. Thus, the resilience indicators R_t and $R_{\%}$ are both scalars between 0 and 1. The resilience indicator R_t indicates the ability of the system to provide a reliable power supply to customers under the malicious attacks, while $R_{\%}$ indicates the overall resilience level of the grid throughout the horizon when the grid is under the impacts of the attacks. A higher R_t indicates a higher resilience level of the power system. When it equals 0, it implies the system is completely interrupted due to the attacks. In contrast, it shows the system is fully able to maintain the power supply to customers under the attacks when R_t is equal to 1.

TABLE I
Key Parameters of Attack and NTO Model

Para.	Value	Para.	Value	Para.	Value
Λ^{CG}	1	τ^{CG}	6 hours	N^{BS}	2
Λ^{CS}	1	τ^{CS}	4 hours	N^{TS}	2
Λ^{P}	2	τ^{P}	24 hours	N^{NTO}	3

Besides the percentage of the demand supplied during the disturbances, another important metric in measuring the power system resilience is how quickly the system can fully recover the power supply to the customers after the beginning of the disturbances. Thus, another resilience indicator $t_{100\%}$ is defined as follows to measure the speed of the system in recovering the power supply after the attacks.

$$t_{100\%} = \inf\{t \mid R_t \geq 100\%,\ t \geq 0\} \tag{45}$$

$t_{100\%}$ indicates the shortest time that is needed by the system to restore all the power supply to the customers after the attack is triggered.

In this study, the resilience indicators R_t, $R_{\%}$ and $t_{100\%}$ are used to assess the power system resilience with the operational strategies of the system operator against the coordinated cyber-physical attacks on the grid.

VI. Case Study

In order to demonstrate the performance of the proposed NTO based model to enhance the resilience of power systems against the coordinated cyber-physical attacks, case studies were conducted on the modified IEEE 57-bus system [33]. The results of the cases studies are presented and discussed in this section. The single line diagram of the IEEE 57-bus system is shown in Fig. 5.

The key parameters of the model in the case studies are listed in Table I.

In the case studies, the proposed coordinated cyber-physical attacks are performed on the test system. In order to demonstrate the performance of the proposed NTO model to enhance the system resilience under the attacks, the proposed NTO based approach is simulated and compared with the conventional optimal power flow (OPF) based optimal redispatch (OR) approach and the optimal transmission switching (OTS) approach. In the OTS approach, only the transmission-switching actions are applied for the power system reconfiguration while the bus-splitting actions are not considered.

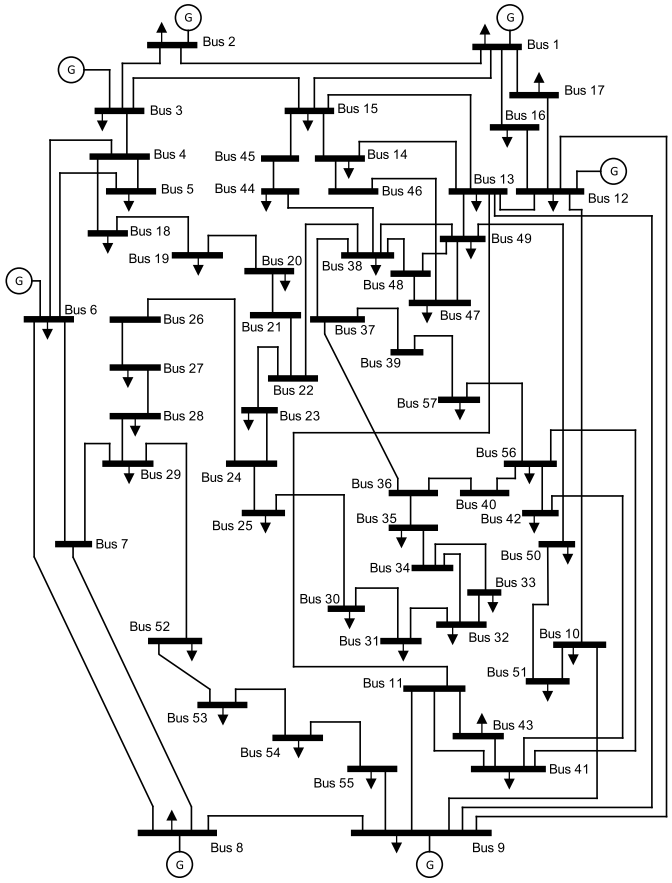


Fig. 5. Single Line Diagram of IEEE 57-bus System.

Denote the time when the coordinated cyber-physical attacks are triggered by $t_0 = 0$, the entire process of the system restoration in the incident can be divided into three stages. Stage I is between t_0 and τ^{CS} when the compromised substations, generation units and transmission branches are all out-of-service. Stage II is between τ^{CS} and τ^{CG} when the compromised substations by the cyberattacks are recovered, while the compromised generation units and transmission branches are yet out-of-service. Stage III is between τ^{CG} and τ^{P} when the compromised generation units by the cyberattacks are also recovered, while the compromised transmission branches are still out-of-service. After τ^{P}, all the components are assumed to be restored. Fig. 6 shows the average load shedding level of the system during each stage and the entire restoration process after the attacks. It is shown that in each stage, the OTS based approach results in a lower load shedding than the conventional OR approach. However, the proposed NTO based approach can further reduce the load shedding level compared with the OTS approach by increasing the flexibility in the system reconfiguration. In Stage I, the case is most serious as the system is most damaged at this stage. There is an about 665 MW load shedding with the conventional OR approach while this number is only around 514 MW with the proposed NTO approach. In Stage II, the case is similar to the trend in Stage I. In Stage III, load shedding is eliminated by the proposed NTO approach while there is still about 84 and 41 MW of load shedding with the conventional OR approach and the OTS approach respectively.

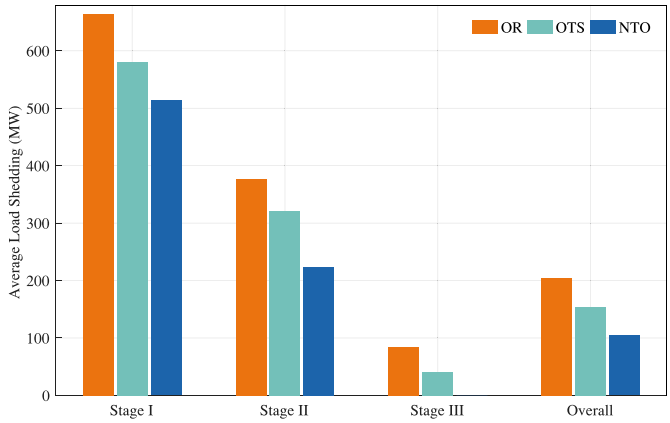


Fig. 6. Average Load Shedding in Different Stages.

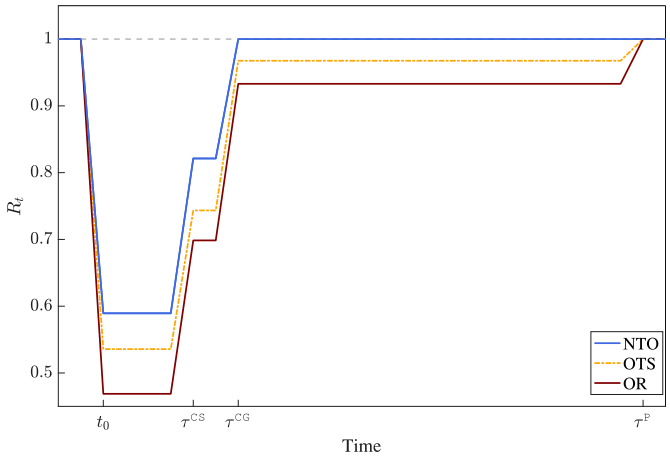


Fig. 7. Resilience Indicator R_t with Different Operation Strategies.

TABLE II
TOTAL LOAD LOSS, RESILIENCE INDICATORS $R_{\%}$ AND $t_{100\%}$

Items	OR	OTS	NTO
Total Load Loss (MWh)	4919.5	3694.7	2501.6
Resilience Indicator $R_{\%}$	83.6%	87.7%	91.7%
Resilience Indicator $t_{100\%}$ (Hour)	24	24	6

Fig. 7 shows the resilience indicator R_t of the system with different operation strategies. It is shown clearly that the resilience indicator R_t with the proposed NTO approach is always higher than the resilience indicator R_t with either the conventional OR approach or the OTS approach. In Stage III, as load shedding is not necessary any more with the proposed NTO approach, $R_t = 1$ consequently, which indicates a cheerful resilience performance of the system with the proposed approach at this stage.

The total load loss, resilience indicators $R_{\%}$ and $t_{100\%}$ in the case studies are listed in Table II. Again, it is clearly shown that the total load loss with the proposed NTO approach is much lower than the load loss with either the conventional OR approach or the OTS approach. The total load loss with the proposed NTO approach is only about 51% of the number with the conventional OR approach and about 68% of that

TABLE III
TOTAL LOAD LOSS (TLL) AND RESILIENCE INDICATORS WITH MODIFIED RESTORATION TIMES FROM BASE CASE

Restoration Time	Items	OR	OTS	NTO
$\tau^{CG} = 4$ hours	TLL (MWh)	4332.8	3133.9	2054.4
	$R_{\%}$	85.6%	89.6%	93.2%
	$t_{100\%}$ (Hour)	24	24	4
$\tau^{CG} = 8$ hours	TLL (MWh)	5506.1	4255.5	2948.8
	$R_{\%}$	81.7%	85.8%	90.2%
	$t_{100\%}$ (Hour)	24	24	8
$\tau^{CS} = 2$ hours	TLL (MWh)	4344.7	3175.1	1921.6
	$R_{\%}$	85.5%	89.4%	93.6%
	$t_{100\%}$ (Hour)	24	24	6
$\tau^{CS} = 6$ hours	TLL (MWh)	5494.2	4214.2	3081.6
	$R_{\%}$	81.7%	86.0%	89.7%
	$t_{100\%}$ (Hour)	24	24	6
$\tau^{P} = 16$ hours	TLL (MWh)	4249.5	3370.3	2501.6
	$R_{\%}$	85.8%	88.8%	91.7%
	$t_{100\%}$ (Hour)	16	16	6
$\tau^{P} = 20$ hours	TLL (MWh)	4584.5	3532.5	2501.6
	$R_{\%}$	84.7%	88.2%	91.7%
	$t_{100\%}$ (Hour)	20	20	6

with the OTS approach. Thus, the overall resilience indicator $R_{\%}$ is increased from about 84% with the conventional OR approach to about 92% by the proposed NTO approach. Moreover, the resilience indicator $t_{100\%}$ is reduced from τ^{P} (which is 24 hours) with the other two approaches to τ^{CG} (which is 6 hours) with the proposed NTO approach. Thus, it is suggested by the results that the system operator can greatly accelerate the recovery of the power supply to the customers with the proposed NTO approach.

In practice, after the attacks are triggered, it may take the system operator a few minutes to hours to identify and locate the compromised targets in the attacks. To recover from the cyberattacks, the system operator may restore the contaminated control systems (e.g., the SCADA systems in substations and power plants) or send staffs to the local stations to switch the operation to manual mode. The duration for this process may take a few hours (e.g., 3 hours in the cyberattack on the Ukrainian power grid in 2015) from the start of the attacks [27], [34], [35]. For the physical damage on the transmission lines in the grid, the repair time may take hours to days according to the experience in the United States and Canada [36], [37]. Thus, the parameters of the restoration times are set as the values shown in Table I in the case study. In order to further validate the proposed model, the cases when the restoration times are different from the base case are also tested, and the results are shown in Table III. As shown in the table, with the increase/decrease of the restoration times, the total load loss and resilience indicators of the grid are worsen/improved respectively. The change of τ^{P} has little impact on the results of the NTO approach as the system operator is able to eliminate the load shedding in the grid before the transmission lines are restored with the NTO model. In all the scenarios, the proposed NTO approach shows less load loss and better resilience metrics compared with the conventional OR and OTS models. Thus, the proposed NTO model is

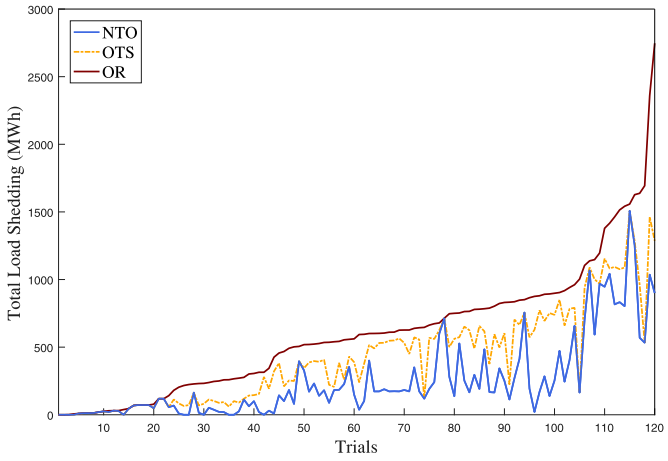


Fig. 8. Total Load Shedding under Random Attack Strategies.

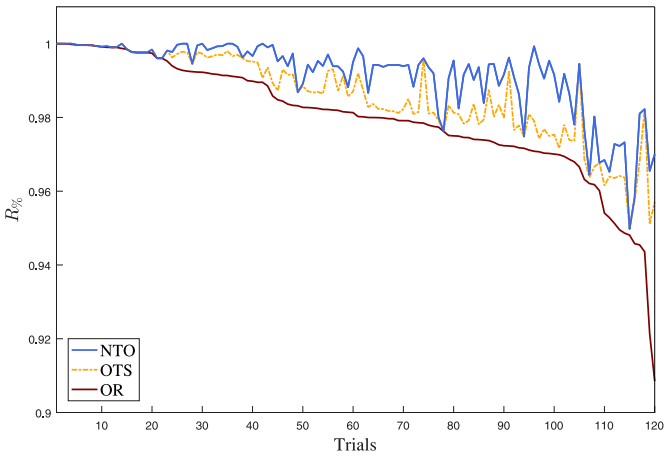


Fig. 9. Resilience Index $R_{\%}$ under Random Attack Strategies.

able to improve the resilience performance of the grid under the cyber-physical attacks.

In order to further demonstrate the performance of the NTO approach in mitigating impacts of the attacks, the cases with random attack strategies were also tested. Figs. 8 and 9 show the total load shedding and $R_{\%}$ with OR, OTS and the proposed NTO approaches in 120 trials where the targets of the cyber-physical attacks were randomly picked. The trials in the figures are sorted in an ascending order of the total load shedding volume with the OR model for a better display. The results show that in every run of the 120 trials, the proposed NTO approach has a better (at least the same) performance in mitigating the impacts of the cyber-physical attacks than the conventional OR and OTS approaches.

To investigate the robustness of the NTO approach, the worst case scenario was tested. It is assumed the attacker knows the NTO based model is in place and tailors the attack strategy so that it can lead to the worst result of the NTO model. The attack strategy can be achieved by replacing the lower level problem of the attack model with the NTO model of the system operator presented in the Appendix. The comparison between the results of the worst case scenario against the NTO approach and the base case is shown in Fig. 10.

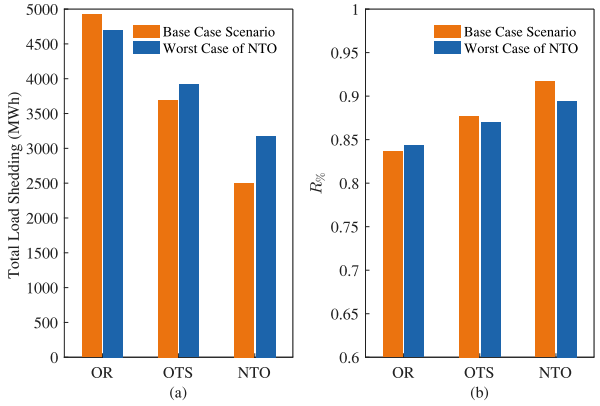


Fig. 10. Comparison between Base Case and Worst Case Scenario against NTO on (a) Total Load Shedding, and (b) Resilience Index $R_{\%}$.

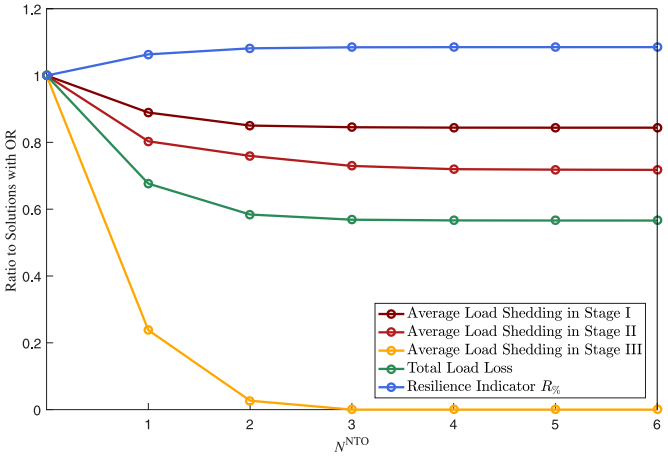


Fig. 11. Impact of N^{NTO} on Performance of the NTO Based Approach.

Compared with the result of the base case, the resilience of the grid with the conventional OR approach is improved while the results of both the OTS and NTO approaches are worsen. However, although the attack scenario is targeting the NTO approach, the performance of the proposed NTO approach still overwhelms the conventional OR and OTS approaches. Less load shedding is caused and better resilience indicator is achieved.

The proposed NTO model is performed after the cyber-physical attack is triggered, and the status of the system components due to the attack is determined and acts as parameters in the NTO model. Thus, the size of the proposed NTO model increases linearly with the size of the grid. Further, the total amount of the transmission-switching and bus-splitting actions is limited, which reduces the computational burden of the problem. In the case study, the proposed NTO model for each case on the 57-bus system in the simulation was solved within 2 seconds using CPLEX on a laptop with Intel Core i5 quad-core CPU (1.60-3.90GHz) and 12GB RAM.

In practice, it is impossible for the system operator to perform a large number of TS and BS actions in the grid. Thus, the impacts of the maximum number of the NTO actions N^{NTO} in the model of the NTO based approach are investigated in the case studies. Fig. 11 shows the ratios of the average load shedding in each stage, total load loss and resilience indicator $R_{\%}$ with the proposed NTO approach to the solutions with the conventional OR approach. When $N^{\mathrm{NTO}} = 0$, no TS or BS actions are allowed in the NTO approach, and it is equivalent to the conventional OR approach. As a result, all the indexes equal 1 when $N^{\mathrm{NTO}} = 0$ as shown in Fig. 11. With the increase of N^{NTO} in the proposed approach, all the indexes share a similar monotonicity. The average load shedding in each stage and the total load loss decrease while the resilience indicator $R_{\%}$ increases with the increase of N^{NTO}. Thus, the resilience of the system is improved with the increase of N^{NTO}. However, it is shown that the resilience of the system increases rapidly with the increase of N^{NTO} and gets saturated very quickly. The numbers of all the indexes are more or less constant when $N^{\mathrm{NTO}} \geq 3$. Thus, the first few NTO actions bring the most value in enhancing the system resilience. While the flexibility introduced by the possibility to perform the TS and BS actions can greatly enhance the system resilience against the attacks, it is less necessary and beneficial to perform a large number of switching actions in the NTO approach.

TABLE IV
TOTAL LOAD LOSS, RESILIENCE INDICATORS $R_{\%}$ AND $t_{100\%}$ IN AN ATTACK SCENARIO ON 118-BUS SYSTEM

Items	OR	OTS	NTO
Total Load Loss (MWh)	2500.1	1704.4	1574.4
Resilience Indicator $R_{\%}$	98.0%	98.6%	98.7%
Resilience Indicator $t_{100\%}$ (Hour)	24	24	6

To further validate the proposed NTO approach in enhancing the resilience of the grid against the cyber-physical attacks, the case study was also conducted on the modified IEEE 118-bus system [38]. The key parameters are the same as the values in the case study on the 57-bus system listed in Table I. Similar to the case on the 57-bus system, the proposed NTO approach outperforms the conventional OR and OTS models in the case on the 118-bus system. Table IV shows the results of an attack scenario on the 118-bus system with the OR, OTS and NTO models. Similar to the case on the 57-bus system, the proposed NTO approach can further reduce the total load shedding of the grid under the cyber-physical attacks compared with the conventional OR and OTS models. Meanwhile, shorter duration of load shedding occurs in the grid with the proposed NTO model. The resilience of the grid against the coordinated cyber-physical attacks is improved.

VII. DISCUSSION

The results of the case studies clearly show the advantages of the proposed NTO approach over the conventional OR and OTS strategies in enhancing the resilience of the grid against the cyber-physical attacks. With the proposed NTO approach, the load shedding of the system is reduced and the necessary time required to eliminate load shedding in the grid is shorten under the attacks. During the restoration process of the system, more and more resources which are down due to the attacks become available to the system operator. However, with the increased flexibility of the system operation provided by the NTO approach, less resources will be needed to provide the power delivery services to the customers in the grid.

Therefore, less load shedding is caused during the restoration process after the attacks are triggered and shorter time is needed to bring the system resilience back to the pre-event state by the NTO approach.

Meanwhile, the results of the case studies show that the first few NTO actions are most valuable in enhancing the system resilience under the cyber-physical attacks on the grid. In the case studies, the volumes of load shedding decrease and the system resilience indexes improve rapidly with the increase of the NTO action amount, and reach the optimal values with a small NTO action amount limit. It is not necessary to perform a large number of transmission-switching and bus-splitting actions in the grid before the load shedding of the system can be reduced and the system resilience is improved. Generally, the number of switching actions is limited in the power system operation. The NTO approach is able to bring most value to the power system resilience enhancement against the cyber-physical attacks even if a large number of switching actions is not allowed in practice.

In the existing literature, defensive islanding and isolation operation are usually used for the proactive actions against the extreme events (e.g., extreme weather-related events). The islanding schemes are also proposed for the efficient restoration of the grid after blackouts. However, the proposed NTO model in this article mainly focuses on the optimal operation of the grid after the coordinated cyber-physical attacks are triggered to minimize the unwanted load shedding in the grid. The compromised components including substations, generation units and transmission branches in the grid are disconnected due to the attacks before the NTO operation is performed. Meanwhile, the proposed NTO model does not aim to partition or split the grid in the operation specifically. Further, generally, the islanding and defensive isolation operation mainly relies on the switching of the transmission lines in the grid. However, the NTO model considers the coordinated transmission-switching and bus-splitting actions in the grid, which further increase the flexibility of the system operation under the attacks.

In the proposed NTO model in this article, the number of switching actions is constrained to model the upper limit of the switching operation amount in the practical operation of the grid. The proposed NTO model in this article aims to minimize the load shedding in the grid, while the number of switching actions is not included in the objective function. However, if the system operator is sensitive to the amount of switching actions in the grid, it can be easily integrated in the proposed NTO model by adding a weighted term of the total number of switching actions in the objective function. The resilience assessment of the grid is evaluated by the performance of the grid in maintaining the power delivery to the customers under the attacks. The impacts of the number of switching actions and the potential of the system reconfiguration on the resilience of the grid is reflected in the results of the system operation under attacks. However, the performance of the grid in maintaining the power delivery to the customers under the attacks is not directly reflected by the number of switching actions. Therefore, the number of switching actions is not used explicitly in the resilience assessment.

VIII. Conclusion

In this article, a bilevel optimization is developed to formulate the coordinated cyber-physical attacks against the power systems. In order to enhance the power system resilience, an NTO based model is proposed to mitigate the impacts of the coordinated cyber-physical attacks on the grid. Resilience metrics are proposed to evaluate the resilience of the system under the attacks. Case studies were conducted on the modified IEEE 57-bus and 118-bus systems. The results of the case studies show that the proposed NTO based approach can effectively mitigate the impacts of the coordinated cyber-physical attacks. The resilience of the power system under attacks is substantially improved by the proposed NTO based approach compared with both the conventional OR based approach and the OTS based approach. The load loss due to the attacks is greatly reduced and the power supply to customers is fully recovered more quickly with the proposed NTO approach. The results also show that the first several NTO actions are the most influential in enhancing the power system resilience, so there is no need to perform a large number of switching actions.

Appendix
Full Formulation of the NTO Model

The full formulation of the NTO based model to mitigate the impacts of the coordinated cyber-physical attacks in Section IV is presented as follows.

$$\min \sum_{i\in\mathcal{N}_v} \delta_{i,t} + \sum_{i\in\mathcal{N}_\varsigma} \left(\delta^{\mathsf{I}}_{i,t} + \delta^{\mathsf{II}}_{i,t}\right) \tag{46}$$

Subject to

$$-M\left(s_{i,j,t} + z_{i,j,t}\right) \le \frac{\vartheta^{\mathsf{Fr}}_{i,j,t} - \vartheta^{\mathsf{To}}_{i,j,t}}{x_{i,j}} - p_{i,j,t},\ \forall i \in \mathcal{N}, (i,j) \in \mathcal{E} \tag{47}$$

$$\frac{\vartheta^{\mathsf{Fr}}_{i,j,t} - \vartheta^{\mathsf{To}}_{i,j,t}}{x_{i,j}} - p_{i,j,t} \le M\left(s_{i,j,t} + z_{i,j,t}\right),\ \forall i \in \mathcal{N}, (i,j) \in \mathcal{E} \tag{48}$$

$$-p^{\mathsf{max}}_{i,j}\left(1 - s_{i,j,t}\right) \le p_{i,j,t} \le p^{\mathsf{max}}_{i,j}\left(1 - s_{i,j,t}\right),\ \forall (i,j) \in \mathcal{E} \tag{49}$$

$$-p^{\mathsf{max}}_{i,j}\left(1 - z_{i,j,t}\right) \le p_{i,j,t} \le p^{\mathsf{max}}_{i,j}\left(1 - z_{i,j,t}\right),\ \forall (i,j) \in \mathcal{E} \tag{50}$$

$$\vartheta^{\mathsf{Fr}}_{i,j,t} = \vartheta_{i,t},\ \forall i \in \mathcal{N}_v, (i,j) \in \mathcal{E} \tag{51}$$

$$\vartheta^{\mathsf{To}}_{i,j,t} = \vartheta_{j,t},\ \forall j \in \mathcal{N}_v, (i,j) \in \mathcal{E} \tag{52}$$

$$-Mw^{\mathsf{Fr}}_{i,j,t} \le \vartheta^{\mathsf{Fr}}_{i,j,t} - \vartheta^{\mathsf{I}}_{i,t} \le Mw^{\mathsf{Fr}}_{i,j,t},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{53}$$

$$-M\left(1 - w^{\mathsf{Fr}}_{i,j,t}\right) \le \vartheta^{\mathsf{Fr}}_{i,j,t} - \vartheta^{\mathsf{II}}_{i,t} \le M\left(1 - w^{\mathsf{Fr}}_{i,j,t}\right),\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{54}$$

$$-Mw^{\mathsf{To}}_{i,j,t} \le \vartheta^{\mathsf{To}}_{i,j,t} - \vartheta^{\mathsf{I}}_{j,t} \le Mw^{\mathsf{To}}_{i,j,t},\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{55}$$

$$-M\left(1 - w^{\mathsf{To}}_{i,j,t}\right) \le \vartheta^{\mathsf{To}}_{i,j,t} - \vartheta^{\mathsf{II}}_{j,t} \le M\left(1 - w^{\mathsf{To}}_{i,j,t}\right),\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{56}$$

$$\sum_{g\in\mathcal{G}_i} p_{g,t} - \left(p_{i,t} - \delta_{i,t}\right) - \sum_{j\in\mathcal{N}:(i,j)\in\mathcal{E}} p_{i,j,t} = 0,\ \forall i \in \mathcal{N}_v \tag{57}$$

$$\sum_{g\in\mathcal{G}_i} p^{\mathsf{I}}_{g,t} - \left(p^{\mathsf{I}}_{i,t} - \delta^{\mathsf{I}}_{i,t}\right) - \sum_{j\in\mathcal{N}:(i,j)\in\mathcal{E}} p^{\mathsf{I}}_{i,j,t} = 0,\ \forall i \in \mathcal{N}_\varsigma \tag{58}$$

$$\sum_{g\in\mathcal{G}_i} p^{\mathsf{II}}_{g,t} - \left(p^{\mathsf{II}}_{i,t} - \delta^{\mathsf{II}}_{i,t}\right) - \sum_{j\in\mathcal{N}:(i,j)\in\mathcal{E}} p^{\mathsf{II}}_{i,j,t} = 0,\ \forall i \in \mathcal{N}_\varsigma \tag{59}$$

$$0 \le p_{g,t} \le p^{\mathsf{max}}_g\left(1 - s_{g,t}\right),\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_v \tag{60}$$

$$0 \le p^{\mathsf{I}}_{g,t} \le p^{\mathsf{max}}_g\left(1 - s_{g,t}\right),\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{61}$$

$$0 \le p^{\mathsf{II}}_{g,t} \le p^{\mathsf{max}}_g\left(1 - s_{g,t}\right),\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{62}$$

$$0 \le \delta_{i,t} \le p_{i,t},\ \forall i \in \mathcal{N}_v \tag{63}$$

$$0 \le \delta^{\mathsf{I}}_{i,t} \le p^{\mathsf{I}}_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{64}$$

$$0 \le \delta^{\mathsf{II}}_{i,t} \le p^{\mathsf{II}}_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{65}$$

$$p^{\mathsf{I}}_{i,t} = p_{i,t}\left(1 - w^{\mathsf{D}}_{i,t}\right),\ \forall i \in \mathcal{N}_\varsigma \tag{66}$$

$$p^{\mathsf{II}}_{i,t} = p_{i,t} w^{\mathsf{D}}_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{67}$$

$$0 \le p^{\mathsf{I}}_{g,t} \le p^{\mathsf{max}}_g\left(1 - w_{g,t}\right),\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{68}$$

$$0 \le p^{\mathsf{II}}_{g,t} \le p^{\mathsf{max}}_g w_{g,t},\ \forall g \in \mathcal{G}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{69}$$

$$-\left(1 - w^{\mathsf{Fr}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j} \le p^{\mathsf{I}}_{i,j,t} \le \left(1 - w^{\mathsf{Fr}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{70}$$

$$-w^{\mathsf{Fr}}_{i,j,t} p^{\mathsf{max}}_{i,j} \le p^{\mathsf{II}}_{i,j,t} \le w^{\mathsf{Fr}}_{i,j,t} p^{\mathsf{max}}_{i,j},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{71}$$

$$-\left(1 - w^{\mathsf{To}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j} \le p^{\mathsf{I}}_{j,i,t} \le \left(1 - w^{\mathsf{To}}_{i,j,t}\right)p^{\mathsf{max}}_{i,j},\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{72}$$

$$-w^{\mathsf{To}}_{i,j,t} p^{\mathsf{max}}_{i,j} \le p^{\mathsf{II}}_{j,i,t} \le w^{\mathsf{To}}_{i,j,t} p^{\mathsf{max}}_{i,j},\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{73}$$

$$p_{i,j,t} = p^{\mathsf{I}}_{i,j,t} + p^{\mathsf{II}}_{i,j,t},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{74}$$

$$p_{i,j,t} = -\left(p^{\mathsf{I}}_{j,i,t} + p^{\mathsf{II}}_{j,i,t}\right),\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{75}$$

$$-Mz_{i,t} \le \vartheta^{\mathsf{I}}_{i,t} - \vartheta^{\mathsf{II}}_{i,t} \le Mz_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{76}$$

$$w^{\mathsf{Fr}}_{i,j,t} \le z_{i,t},\ \forall i \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{77}$$

$$w^{\mathsf{To}}_{i,j,t} \le z_{j,t},\ \forall j \in \mathcal{N}_\varsigma, (i,j) \in \mathcal{E} \tag{78}$$

$$w_{g,t} \le z_{i,t},\ \forall i \in \mathcal{N}_\varsigma,\ \forall g \in \mathcal{G}_i \tag{79}$$

$$w^{\mathsf{D}}_{i,t} \le z_{i,t},\ \forall i \in \mathcal{N}_\varsigma \tag{80}$$

$$\sum_{i\in\mathcal{N}_\varsigma} z_{i,t} \le N^{\mathsf{BS}} \tag{81}$$

$$\sum_{(i,j)\in\mathcal{E}} z_{i,j,t} \le N^{\mathsf{TS}} \tag{82}$$

$$\sum_{i\in\mathcal{N}_\varsigma} z_{i,t} + \sum_{(i,j)\in\mathcal{E}} z_{i,j,t} \le N^{\mathsf{NTO}} \tag{83}$$

$$w^{\mathsf{I}}_{i,b,t} \le w^{\mathsf{II}}_{i,b,t},\ \forall b \in \mathcal{B}_i,\ \forall i \in \mathcal{N}_\varsigma \tag{84}$$

where constraints (60)–(62) are the power constraints of the generation units based on their statuses in the restoration processes after the attacks. Constraints (77)–(80) ensure that the transmission branches, generation units and load at one substation can only be connected to two independent busbars when a BS action is performed in the corresponding substation. In practice, the maximum numbers of the NTO actions are limited. Thus, it is constrained as (81)–(83). The NTO based model is performed by minimizing (46) subject to (47)–(83). When the breaker-and-a-half configuration is employed in the substations, constraint (84) should be added into the model.

REFERENCES

[1] M. Assante *et al.*, "High-impact, low-frequency event risk to the North American bulk power system," North Amer. Elect. Rel. Corp. (NERC), Atlanta, GA, USA, Rep., Jun. 2010.

[2] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, Dec. 2017.

[3] Reliability Issues Steering Committee (RISC), "Reliability issues steering committee report on resilience," North Amer. Elect. Rel. Corp. (NERC), Atlanta, GA, USA, Rep., Nov. 2018.

[4] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power systems resilience assessment: Hardening and smart operational enhancement strategies," *Proc. IEEE*, vol. 105, no. 7, pp. 1202–1213, Jul. 2017.

[5] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyiou, "Metrics and quantification of operational and infrastructure resilience in power systems," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4732–4742, Nov. 2017.

[6] G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, "Integration of preventive and emergency responses for power grid resilience enhancement," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4451–4463, Nov. 2017.

[7] C. Wang, Y. Hou, F. Qiu, S. Lei, and K. Liu, "Resilience enhancement with sequentially proactive operation strategies," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2847–2857, Jul. 2017.

[8] C. Shao, M. Shahidehpour, X. Wang, X. Wang, and B. Wang, "Integrated planning of electricity and natural gas transportation systems for enhancing the power grid resilience," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4418–4429, Nov. 2017.

[9] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the power grid resilience to extreme weather events using defensive islanding," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2913–2922, Nov. 2016.

[10] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266, Jul. 2017.

[11] S. Soltan, P. Mittal, and H. V. Poor, "Line failure detection after a cyber-physical attack on the grid using Bayesian regression," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3758–3768, Sep. 2019.

[12] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[13] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2016–2025, Jul. 2016.

[14] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[15] H. M. Chung, W. T. Li, C. Yuen, W. H. Chung, Y. Zhang, and C. K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019.

[16] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[17] E. J. Oughton *et al.*, "Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks on electricity distribution infrastructure networks," *Risk Anal.*, vol. 39, no. 9, pp. 2012–2031, Sep. 2019.

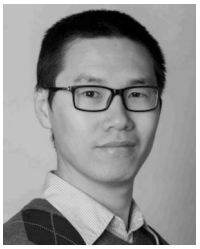
[18] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096–7108, Nov. 2018.

[19] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "On data integrity attacks against real-time pricing in energy-based cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 1, pp. 170–187, Jan. 2017.

[20] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Trans. Inf. Forensics Security*, vol. 9, pp. 2340–2354, 2014.

[21] Å. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 76–84, Feb. 2007.

[22] Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.
[23] M. Heidarifar and H. Ghasemi, "A network topology optimization model based on substation and node-breaker modeling," *IEEE Trans. Power Syst.*, vol. 31, no. 1, pp. 247–255, Jan. 2016.
[24] R. Xiao, Y. Xiang, L. Wang, and K. Xie, "Power system reliability evaluation incorporating dynamic thermal rating and network topology optimization," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6000–6012, Nov. 2018.
[25] Y. Li *et al.*, "Day-ahead scheduling of power system incorporating network topology optimization and dynamic thermal rating," *IEEE Access*, vol. 7, pp. 35287–35301, 2019.
[26] ISO New England Planning Procedure, "Major substation bus arrangement requirements and guidelines," ISO New England (ISO-NE), Holyoke, MA, USA, Rep. PP9, Sep. 2017.
[27] A. Shehod, "Ukraine power grid cyberattack and U.S. susceptibility: Cybersecurity implications of smart grid advancements in the U.S.," Dept. Cybersecurity Interdiscipl. Syst. Lab., Massachusetts Inst. Technol., Cambridge, MA, USA, Rep. CISL-2016-22, 2016.
[28] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Prot. Relay Eng. (CPRE)*, College Station, TX, USA, Apr. 2017, pp. 1–8.
[29] Y. Yang, H. Xu, L. Gao, Y. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.
[30] M. Morgan *et al.*, *Terrorism and the Electric Power Delivery System*. Washington, DC, USA: Nat. Acad. Press, 2012.
[31] M. Ouyang, L. Dueñas-Osorio, and X. Min, "A three-stage resilience analysis framework for urban infrastructure systems," *Struct. Safety*, vols. 36–37, pp. 23–31, May/Jul. 2012.
[32] H. H. Willis and K. Loa, "Measuring the resilience of energy distribution systems," RAND Corp., Santa Monica, CA, USA, Rep. RR883, 2015.
[33] R. Christie, "IEEE 57-bus power flow test case," Univ. Washington, Seattle, WA, USA, Aug. 1993. [Online]. Available: https://egriddata.org/dataset/ieee-57-bus-power-flow-test-case
[34] V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Security of SCADA systems against cyber–physical attacks," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 5, pp. 28–45, May 2017.
[35] R. D. Larkin, J. J. Lopez, J. W. Butts, and M. R. Grimaila, "Evaluation of security solutions in the SCADA environment," *Data Base Adv. Inf. Syst.*, vol. 45, no. 1, pp. 38–53, Mar. 2014.
[36] C. Grigg *et al.*, "The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.
[37] *Underground Transmission Lines*, DATC.com. Charlotte, NC, USA, 2013. [Online]. Available: https://www.datcllc.com/learn/underground-transmission
[38] R. Christie, *Power Systems Test Case Archive: 118 Bus Power Flow Test Case*, Univ. Washington, Seattle, WA, USA, May 1993. [Online]. Available: http://labs.ece.uw.edu/pstca/pf118/pg_tca118bus.htm



Zhaoxi Liu (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 2006 and 2008, respectively, and the Ph.D. degree in electrical engineering from the Technical University of Denmark, Denmark, in 2016.

He is currently a Research Associate with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee, WI, USA. His research interests include power system operation, integration of renewable energy and distributed energy resources in power systems, and power system security and resiliency.

Lingfeng Wang (Senior Member, IEEE) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997, the M.S. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2002, and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University, College Station, TX, USA, in 2008.

He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee (UWM), Milwaukee, WI, USA. His major research interests include power system reliability and security and resiliency. He was a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018. He is an Editor of the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and served on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING.