# Vulnerability Analysis of Power Systems Under Physical Deliberate Attacks Considering Geographic-Cyber Interdependence of the Power System and Communication Network

Mehdi Zeraati, *Student Member, IEEE*, Zahra Aref, and Mohammad Amin Latify

***Abstract*—This paper addresses the vulnerability of the power system subjected to physical deliberate attacks (PDAs) when the power system and communication network are geographic-cyber interdependent. This interdependence is due to the use of the transmission line towers as an available infrastructure to establish the communication network that controls the power system. The attacker plans a PDA on both transmission lines and the communication network to damage the power system, and in reverse the system operator (SO) reacts as a defender by taking necessary actions against them. To this end, a bilevel optimization based model is presented. The upper level problem formulates the attacker's problem with the objective function of maximizing damage inflicted on the power system through the simultaneous PDA on the transmission lines and communication links. In the lower level, the SO's problem is modeled with the objective function of minimizing damage to the system through the corrective actions including the change in the production level of generation units and the load shedding. The SO's corrective actions are performed through a main intact connected communication network and the alternative infrastructure according to the power system operation strategy in emergency. For the proposed bilevel model, a solution approach is proposed based upon the combination of the genetic algorithm and mixed integer linear programming. Finally, numerical results obtained by implementing the model on the 24-bus IEEE reliability test system are presented and then compared with previous studies. The efficacy of the proposed model is confirmed by different numerical case studies.**

***Index Terms*—Bilevel optimization, deliberate attacks, geographic-cyber interdependence, vulnerability.**

## Nomenclature

*Indices and Sets*

| | |
|---|---|
| $d$ | Load index. |
| $g$ | Generation unit index. |
| $l$ | Transmission line index. |
| $n$ | Bus index. |
| $\Omega_D$ | Set of indices of loads. |
| $\Omega_G$ | Set of indices of generation units. |
| $\Omega_L$ | Set of indices of transmission lines. |
| $\Omega_N$ | Set of indices of buses. |

*Parameters*

| | |
|---|---|
| $A_{nd}^D$ | Incidence of load $d$ and bus $n$ (equals 1 if the load and the bus are connected, otherwise 0). |
| $A_{ng}^G$ | Incidence of generation unit $g$ and bus $n$ (equals 1 if the generation unit and the bus are connected, otherwise 0). |
| $A_{nl}^L$ | Incidence of transmission line $l$ and bus $n$ (equals 1 if the bus is the sending bus of line, $-$ 1 if the bus is the receiving bus of line, otherwise 0). |
| $P_d^D$ | Demand of load $d$ (MW). |
| $P_g^G$ | Initial output power of generation unit $g$ (MW). |
| $P_{l,\max}^F$ | Power flow capacity of line $l$ (MW). |
| $R$ | Maximum number of attacked lines. |
| $X_l^L$ | Reactance of line $l$ (p.u.). |
| $\alpha, \beta$ | Weighting coefficients in the objective function. |
| $\Delta P_{g,\text{inc}}^G$ | Maximum power increase of generation unit $g$ (MW). |
| $\Delta P_{g,\text{dec}}^G$ | Maximum power decrease of generation unit $g$ (MW). |

*Variables*

| | |
|---|---|
| $LS_d^D$ | Load shedding of load $d$ (MW). |
| $P_l^F$ | Power flow of line $l$ (MW). |
| $\Delta P_g^G$ | Output power change of generation unit $g$ (MW). |
| $\Delta P_g^{G,\text{Con}}$ | Output power change of communication-connected generation unit $g$ (MW). |
| $\Delta P_g^{G,\text{Dis}}$ | Output power change of communication-disconnected generation unit $g$ (MW). |
| $W_d^D$ | Binary variable corresponding to load $d$ connectivity (equals 1 if load $d$ is communication connected and 0 otherwise). |
| $W_g^G$ | Binary variable corresponding to generation unit $g$ connectivity (equals 1 if generation unit $g$ is communication connected and 0 otherwise). |
| $Y_g^G$ | Binary variable corresponding to generation unit $g$ shut down (equals 0 if generation unit $g$ is shut down and 1 otherwise). |
| $Z_l^L$ | Binary variable of transmission line $l$ connectivity (equals 0 if line $l$ is attacked and 1 otherwise). |
| $\theta_n^N$ | Phase angle of bus $n$ (rad). |

Manuscript received November 24, 2016; revised April 19, 2017; accepted September 30, 2017. *(Corresponding author: Mohammad Amin Latify.)*

The authors are with the Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran (e-mail: m.zeraati@ec.iut.ac.ir; z.aref@ec.iut.ac.ir; latify@cc.iut.ac.ir).

Digital Object Identifier 10.1109/JSYST.2017.2761844

## I. Introduction

### A. Motivation

The minimization of the vulnerability of critical infrastructures and the increase in their resilience is one of the most important programs in European Union. It is obligated to reach an optimal level of protection and restrict the adverse effects of disruptions on the society and citizens as far as possible. A general framework for activities is adjusted by the European programme for critical infrastructure protection [1], which is aimed at improving the protection of the critical infrastructure such as the power system. Moreover, the national infrastructure protection plan [2] in the USA is associated with the risk management of its critical infrastructures. Therefore, the vulnerability assessment of critical infrastructures is of great importance.

The development of the smart grids has accelerated the growth of communication infrastructures in power systems, which would lead to enhanced efficiency [3]. Nevertheless, the subsequent interdependence between the power system and communication network potentially creates more risk; as, a failure in one infrastructure can cause a failure in other infrastructures, which can create system-wide outages [4], [5]. The analysis of extensive blackouts in recent years has concluded that the main reason of such incidents is associated to a disconnected communication network from the power system operator (SO) [6]. Therefore, investigating the impact of a communication network on vulnerability of a power systems is necessary.

In recent years, due to some economic, political, and environmental issues, the power systems have not been developed proportional to the demand growth. Hence, often times, they are operated close to static and dynamic operation limits [7]. As such, the vulnerability of power systems has increased as it is confirmed by extensive amounts of recent blackouts. The high vulnerability and geographic extent of the power systems make them more likely targets for physical deliberate attacks (PDAs) [4]. Thus, the analysis of the vulnerability of power systems to PDAs is a constructive open-field research topic.

The research works on PDAs show that attackers gain access to a large amount of information. Hence, PDAs are generally launched through the use of sufficiently complete information and minimal resources by the attacker who aims to maximize the damage to available infrastructures [4]. Therefore, PDAs can be designed such that the potential weaknesses caused by the interdependence of power systems and communication networks are exploited. Since when a PDA is launched simultaneously at both transmission lines and communication links, it may cause more load shedding than occurring at only transmission lines. This difference is due to the loss of communication links and the subsequent disconnection between the SO and system components. So, it is necessary to propose a model to study the vulnerability of the power system, dependent to the communication network, to PDAs.

### B. Methodology

In theory, the interdependence of infrastructures is classified into four groups [5], namely geographic, cyber, physical, and logical interdependence. In this paper, we study the geographic and cyber interdependence of power systems and their communication networks. Geographic interdependence is primarily developed by using a fiber-optic network as a high-speed communication infrastructure in order to control the power system and implement the wide-area measurement system. Transmission line towers are one of the cost effective and commonly used facilities for the construction and further development of the fiber-optic network that, in turn, leads to the geographic interdependence. The fiber-optic network is usually installed parallel with transmission lines and laid on transmission towers. Thus, a PDA on one infrastructure (transmission lines) can influence the other (communication links).

The cyber interdependence exists, as operating instructions and control signals in power system are communicated via the communication network. Therefore, the communication network's disruption due to PDAs can lead to the risks in the power system operation. Nevertheless, some alternative communication networks are considered in operation strategies in emergency situation (OSEs), which are established with delay [8].

In this paper, we propose a model that assesses the vulnerability of power systems to PDAs by considering the geographic-cyber interdependence of the power system and communication network. An attacker–defender (AD) model is developed based upon the bilevel optimization approach. This model extends the approach introduced by [9]. It is assumed in [9] that the SO issues the corrective postattack instructions for generation units and load buses throughout the power system without any delay and disruption, since the effect of the communication network on the SO's response is not considered. However, the SO's postattack instructions will be inevitable to some delay and may be even disrupted.

In the upper level, the attacker's problem is modeled as an optimization problem with the objective function of maximizing the damage to the power system. The PDA to the power system, simultaneous with the communication network, is considered as the upper level decision variable. In the case of a PDA on the transmission line, both the transmission and communication links will be lost at once. The transmission lines outages can directly lead to the load shedding. Further, the loss of communication links may lead to a disconnected communication network, and thus loss of control over some parts of the power system, that will indirectly result in more load shedding. The adverse effects of simultaneous attacks on two infrastructures are considered in this paper.

In the lower level, SO optimization problem is modeled as a defender model. The objective function of the SO is to minimize the adverse impacts of PDAs on operation. Decision variables of the problem are the amount of load shedding and the changes in the production level of generation units that are connected through the main communication network or an alternative communication network. OSE gives specific instructions to utilize an alternative communication network. Thus, SO aims at minimizing the damage inflicted on the power system through the decision variables as per the instructions presented in OSEs. To this end, two common strategies are introduced in Section II.

The lower level model constraints include the operation constraints of those parts of the power system and communication

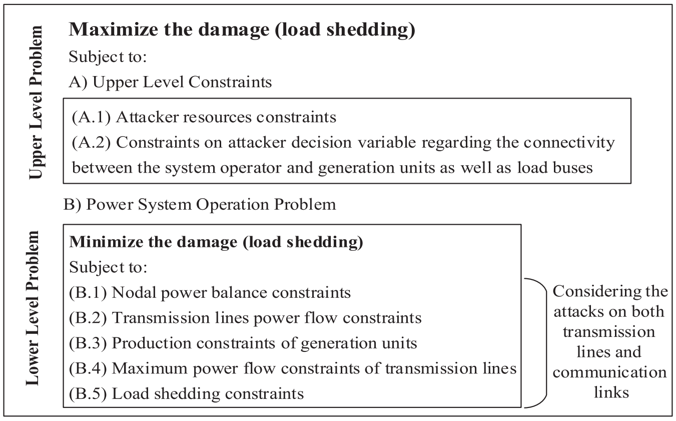
Upper Level Problem
**Maximize the damage (load shedding)**
Subject to:
A) Upper Level Constraints
(A.1) Attacker resources constraints
(A.2) Constraints on attacker decision variable regarding the connectivity between the system operator and generation units as well as load buses
B) Power System Operation Problem
Lower Level Problem
**Minimize the damage (load shedding)**
Subject to:
(B.1) Nodal power balance constraints
(B.2) Transmission lines power flow constraints
(B.3) Production constraints of generation units
(B.4) Maximum power flow constraints of transmission lines
(B.5) Load shedding constraints
Considering the attacks on both transmission lines and communication links

Fig. 1. Proposed bilevel model.

networks that are not disrupted and also are influenced by utilizing an alternative communication network (see Section II).

A novel solution method is developed based on a combination of the genetic algorithm (GA) and mixed integer linear programming (MILP) and is fully described in Section IV.

### *C. Literature Review and Contributions*

Different aspects of the vulnerability of power systems to PDAs are discussed in the literature [10]–[17]. Power system's vulnerability is analyzed in [10] using extended topological metrics by incorporating several electrical features. The effects of PDAs on operational capability of the transmission system are quantified in [11]. The mathematical formulation of the power system security against PDAs is developed as an AD problem that identifies the critical components of a power system in [12]. The bilevel programming based formulation presented in [12] is converted to an MILP model in [13]. A new bilevel programming problem is also developed in [14], in which the objective of the attacker is to determine the minimum number of PDAs while expecting a minimum amount of load to be shed. Vulnerability of power systems under multiple contingencies is analyzed in [9], which provides a minimum vulnerability as well as a maximum model. The first model determines the minimum number of simultaneous PDAs on transmission lines with the goal of reaching a load shedding greater than or equal to a predefined value. However, in the second one, the maximum load shedding is specified by a number of targeted lines less than or equal to a given value. A game theoretical framework is developed in [15] to find and evaluate new approaches to defend the electric power system against PDAs. In [16], a bilevel programming based vulnerability analysis problem is developed to consider the transmission line switching as one of the most effective actions taken by the SO to reinforce the system against PDAs. Bilevel programming based model proposed in [17] is able to determine the best locations and the best times, simultaneously, for launching PDAs.

The vulnerability analysis of power systems dependent on communication networks is investigated in [6] and [18]–[25]. To assess the direct impacts of cyber-power interdependencies on the reliability of the power system, two optimization problems are introduced in [6]. The problems are modeled to maximize the data connection while minimizing the amount of load shedding to evaluate the reliability indices. The impacts of indirect cyber-power interdependencies are discussed in [18]. In [19], the vulnerability caused by the coordination between physical (deliberate outages of transmission lines) and cyber attacks (false data injection) is analyzed. In [20], a certain type of false data injection in order for load redistribution is developed, and also its effect on the power system operation is analyzed. In [21], a methodology is presented to reliably detect the attacks in cyber-physical critical infrastructures. A framework for modeling the interdependence of physical and cyber systems as well as identifying their weak points is introduced in [22], which evaluates the reliability of these infrastructures. In [23], an integrated model for the cyber and physical vulnerability analysis of a power system and the associated communication network through the use of incomplete information is provided. In this regard, it applies a graph theory based method. A criterion for the cyber-physical security assessment is introduced in [24] to manage the risk to the power systems. This effectively reveals the progress of malicious attacks. A cyber-physical vulnerability evaluation technique under accidental contingencies and malicious attacks is suggested in [25].

The significance of our study and the contributions added to the current literature are provided as follows.

1) To provide a bilevel optimization based model, which assesses the vulnerability of a power system considering the geographic-cyber interdependencies of the power system and communication network.
2) To model the simultaneous PDA on the power system and communication network.
3) To introduce an approach to solve the proposed vulnerability analysis problem.
4) To model the two common power system OSEs under the PDAs.

### *D. Paper Organization*

This paper is organized as follows. In Section II, the model is described that is also followed by the two different power system OSEs. In Section III, the mathematical formulation is developed. The solution method is explained in Section IV. In Section V, the numerical results are provided, and Section VI is devoted to drawing the conclusions.

## II. Model Description

The model is depicted in Fig. 1. Since transmission lines are the most likely target compared to other components in a power system, we focus on the PDAs on transmission lines [14].

The objective of the upper level problem is set to maximize the amount of load shedding. The upper level decision variable is defined as the PDAs on the transmission lines. Due to limited resources of an attacker [19], a constraint is introduced that keeps the number of PDAs within limits, which is shown as constraint A.1. In case of a PDA, it will likely result in an out of service communication link and thus a disconnected SO from several components of the power system. Consequently, it is necessary to execute the instructions of OSE throughout the disconnected areas. Therefore, the attacker's plan to interrupt a transmission line, with regards to the issues addressed above, is also modeled as constraint A.2.

The SO attempts to minimize the damage on the power system using all the available resources subject to the power system operation constraints. Hence, the attacker considers some possible responses from the SO. As a result, the second set of constraints is introduced as an operation optimization problem that is expressed through constraints B.

Accordingly, the decision variables in the lower level problem are quantified by the adjustment of production at generation units and also by the load shedding applied in different buses of the network. Such decision variables can be utilized through an intact connected communication network. According to the OSE (e.g., Pennsylvania, New Jersey, and Maryland (PJM) operation manual [8] and Iran grid management company (IGMC) operation manual [26]), main communication network can be substituted by the alternative communication infrastructures when it is disconnected. Hence, regardless of any unavoidable delay, alternative communication infrastructures will, to some extent, improve the results of corrective actions. In this paper, two OSEs are considered to investigate the adverse impacts of deliberate outages of the main communication links, which are further explained in the following.

1) *OSE A (The Delayed Response of the Disconnected Components)*: Since it is somewhat impractical to issue the instructions to communication-disconnected components through the main communication network, an alternative communication infrastructure should be provided. Some OSEs (e.g., in PJM) force the SO to send instructions through satellite and cell phones in order of priority, when a communication link is lost [27]. Hence, the SOs' reaction is inevitable to some delay.
2) *OSE B (Shutting Down Disconnected Generation Units)*: In emergency, some generation units are more likely to suffer from frequency deviations due to the overload or overproduction. In this case, to avoid the damage, some generation units are shut down by underfrequency or overfrequency relays (as instructed by PJM and IGMC OSEs) [28], [29]. This strategy is generally implemented through SO and also automatically controlled relays. The relays are set such that once the frequency violates the authorized limit, they just operate and thus shut down the corresponding generation units. Therefore, to model this strategy, in case of the communication disconnection, the generation units' production is tried to be kept at the same level as those of prior to the attack, and otherwise, it is shut down.

The lower level constraints are expressed in B.1–B.5 in Fig. 1, which is taken similar to the traditional dc optimal power flow constraints [30]. These are modeled differently according to the transmission lines and communication links outages as well as the OSE.

## III. Mathematical Formulation

### A. Upper Level Problem

The maximum vulnerability model, introduced by [9], is modified and adjusted to consider the effect of communication links, as explained in the following. Model (1)–(5) shows the mathematical representation of the upper level problem

$$\max_{\overline{Z}^L} \sum_{d\in\Omega_D} LS_d^D \tag{1}$$

subject to

$$\sum_{l\in\Omega_L} (1-\overline{Z}^L) \leq \ R \tag{2}$$

$$Z_l^L \ \in \ \{0,1\} \quad \forall l \in \Omega_L \tag{3}$$

$$\overline{W}^G \ = \ f(\overline{Z}^L) \tag{4}$$

$$\overline{W}^D \ = \ h(\overline{Z}^L) \tag{5}$$

where, (1) represents the objective function that is to maximize the sum of the load-shedding amount, (2) identifies an upper limit for the number of attacks, and the upper level decision variables are expressed with a binary vector $\overline{Z}^L$ in (3). In case of an attack on line $l$, element $l$ of $\overline{Z}^L (Z_l^L)$ is set to be 0 and otherwise, it equals 1. Two vectors of binary variables $\overline{W}^G$ and $\overline{W}^D$ are introduced that determine the status of communication paths between the SO and generation units as well as load buses, respectively. These are functions ($f$ and $h$) of the decision vector $\overline{Z}^L$. The functions $f$ and $h$ are calculated according to the method given in Section IV. The associated element to a generation unit in $\overline{W}^G$ is equal to 1 if there is still a communication path between the SO and that generation unit in a PDA scenario, otherwise it is set to be 0. Similarly, $\overline{W}^D$ is defined for load buses.

### B. Lower Level Problem: OSE A

The formulation for the problem is given in the following:

$$LS_d^D \in \arg\Big\{ \min_{\overline{\theta}^N, |\overline{\Delta P}^G|, \overline{P}^F, \overline{LS}^D} \sum_{d\in\Omega_D} W_d^D LS_d^D \\ + \alpha \sum_{d\in\Omega_D} (1-W_d^D) LS_d^D + \beta \sum_{g\in\Omega_G} (1-W_g^G)|\Delta P_g^G| \tag{6}$$

subject to

$$\sum_{g\in\Omega_G} A_{ng}^G (P_g^G + \Delta P_g^G) - \sum_{l\in\Omega_L} A_{nl}^L P_l^F \\ = \sum_{d\in\Omega_D} A_{nd}^D (P_d^D - LS_d^D) \quad \forall n \in \Omega_N \tag{7}$$

$$P_l^F = Z_l^L \frac{1}{X_l^L} \sum_{n\in\Omega_N} A_{nl}^L \theta_n^N \quad \forall l \in \Omega_L \tag{8}$$

$$\Delta P_{g,\mathrm{dec}}^G \leq \Delta P_g^G \leq \Delta P_{g,\mathrm{inc}}^G \quad \forall g \in \Omega_G \tag{9}$$

$$-P_{l,\max}^F \leq P_l^F \leq P_{l,\max}^F \quad \forall l \in \Omega_L \tag{10}$$

$$0 \leq LS_d^D \leq P_d^D \quad \forall d \in \Omega_D \Big\} \quad \forall d \in \Omega_D \tag{11}$$

where (6) is the objective function that is comprised of three terms. The first term identifies the load shedding amount issued by the SO in those load buses capable of communicating via the main communication network. The second term represents the amount of load shedding in the communication-disconnected load buses and the third term represents the change in the production of the communication-disconnected generation units. These are expressed by weighting coefficients $\alpha$ and $\beta$, respectively. $|...|$ indicates the absolute value. This is used in the objective function due to the fact that it makes no difference to SO to increase or reduce the production level at generation units in terms of the cost.

Constraint (7) represents the nodal power balance, which ensures the balance of generation, load, and power flows at any given bus of the power system. Equation (8) shows the power flow of line $l$ depending on the attack status ($Z_l^L = 0, 1$). In constraint (9), the change in generation units' production from that of before attack ($P_g^G$) is forced to be within the predefined limits. Constraint (10) expresses the line flow capacity. Constraint (11) represents the boundaries of an authorized load shedding at a load bus.

To describe how the delayed communication via an alternative infrastructure is modeled, assume that none of the communication paths are interrupted by an attack (i.e., $W_d^D = 1, W_g^G = 1 \quad \forall d, g$). The problem is similar to the model introduced in [9]. Now, assume that only the communication path between bus $d_1$ and the SO is interrupted by an attack. The objective function yields to be $\sum_{\substack{d\in\Omega_D \\ d\neq d_1}} LS_d^D + \alpha LS_{d_1}^D$, in which $\alpha$ weighs the increase of load shedding of bus $d_1$ compared to the other buses. With some high values of $\alpha$, the optimization model (6)–(11) solves the problem with the minimum use of load shedding at bus $d_1$. It means that the power system operation problem in case of an attack should be solved by means of decision variables in communication-connected areas, if possible. Otherwise, the decision variable in disconnected area ($LS_{d_1}^D$) is utilized. In this way, the impact of the delay in establishing a communication link with the disconnected bus is modeled. Further, $\beta$ can be interpreted similarly.

In reality, $\alpha$ and $\beta$ vary based upon the generation units and the load buses conditions, but to simplify, it is assumed that all coefficients associated with the load buses are equal to each other and the same is set for those of related to generation units. $\alpha$ and $\beta$ are considered to be different. This is due to the fact that in most of OSEs, it is recommended that in case of frequency increase, the load must be immediately shed at load buses step by step, whereas the generation units should further tolerate the frequency increase, which results in more delays in response.

It should be noted that determining the values of $\alpha$ and $\beta$ is generally based on the characteristics of the power system (e.g., operation instructions, available communication infrastructures, and the dynamic response of components), which is beyond the scope of this paper.

### *C. Lower Level Problem: OSE B*

The formulation for the problem is given in the following:

$$LS_d^D \in \arg\Big\{ \min_{\overline{\theta}^N, \overline{P}^F, \overline{LS}^D, \overline{Y}^G} \sum_{d\in\Omega_D} W_d^D LS_d^D + \alpha \sum_{d\in\Omega_D} (1 - W_d^D) LS_d^D + \beta \sum_{g\in\Omega_G} (1 - Y_g^G)(1 - W_g^G) P_g^G \tag{12}$$

subject to

$$\sum_{g\in\Omega_G} W_g^G A_{ng}^G (P_g^G + \Delta P_g^{G,\text{Con}}) + (1 - W_g^G) A_{ng}^G (\Delta P_g^{G,\text{Dis}}) - \sum_{l\in\Omega_L} A_{nl}^L P_l^F = \sum_{d\in\Omega_D} A_{nd}^D (P_d^D - LS_d^D) \quad \forall n \in \Omega_N \tag{13}$$

$$0 \leq Y_g^G \leq 1 - W_g^G \quad \forall g \in \Omega_G \tag{14}$$

$$P_l^F = Z_l^L \frac{1}{X_l^L} \sum_{n\in\Omega_N} A_{nl}^L \theta_n^N \quad \forall l \in \Omega_L \tag{15}$$

$$W_g^G \Delta P_{g,\text{dec}}^G \leq \Delta P_g^{G,\text{Con}} \leq W_g^G \Delta P_{g,\text{inc}}^G \quad \forall g \in \Omega_G \tag{16}$$

$$\Delta P_g^{G,\text{Dis}} = Y_g^G P_g^G \quad \forall g \in \Omega_G \tag{17}$$

$$- P_{l,\max}^F \leq P_l^F \leq P_{l,\max}^F \quad \forall l \in \Omega_L \tag{18}$$

$$\left. 0 \leq LS_d^D \leq P_d^D \quad \forall d \in \Omega_D \right\} \quad \forall d \in \Omega_D. \tag{19}$$

The objective function is expressed in (12) where the terms are interpreted as those of (6). Equation (13) represents the nodal power balance. The logic behind the "shutting down" state of disconnected generation units is imposed by constraints (14). Constraints (15), (18), and (19) are identical to (8), (10), and (11), respectively. Constraints (16) and (17) introduce the constraints on generation adjustment at communication-connected and -disconnected generation units, respectively.

To clarify how OSE B is implemented, assume that the communication path between the generation unit $g_1$ and the SO is interrupted subsequent to an attack on transmission lines (i.e., $W_d^D = 1 \quad \forall d, W_g^G = 1 \quad \forall g \neq g_1, 0 \leq Y_g^G \leq 1 \quad \forall g = g_1, Y_g^G = 0 \quad \forall g \in \Omega_G / g = g_1$). The objective function (12) minimizes the amount of load to be shed at all communication-connected buses as well as the changes in the production level of generation unit $P_{g_1}^G$, which takes into account the response delay factor $\beta$. The constraint (16) expresses that the adjustment of production in generation units (with the exception of $g_1$) can continuously vary within the permitted limits. Nevertheless, the production of generation unit $g_1$ is restricted to values of $P_{g_1}^G$ and zero [as can be drived by (17)], which is determined by the binary variable $Y_{g_1}^G$ based on the needs of the objective function. Due to the large value of $\beta$, at first, the model attempts to find the solution by adjusting the production of the communication-connected generation units and also by shedding load at the communication-connected buses. If a feasible solution cannot be reached, it eventually achieves the solution by shutting the generation unit $g_1$ down ($Y_{g_1}^G = 0$). In fact, this occurs as underfrequency or overfrequency relays operate. Unit $g_1$ will be shut down with a delay according to its relay function. In this way, the delay of generation unit $g_1$, in response to the event considering OSE B, is modeled.

The only difference between OSE B and OSE A is that through OSE B the communication-disconnected generation units might run out of service prior to be connected via the alternative communication network. This occurs due to the fact that underfrequency or overfrequency relays may redress the imbalance between the production and consumption in the power system in emergency and thus protect the generation units through shutting them down. Therefore, only the last term of the objective function is modified in comparison with (6). In fact, rather than causing a delay due to changing the set point of communication-disconnected generation units, they must either continue the operation at the preattack set point or be switched OFF depending on the state of the system. To this end, the decision variable $Y_g^G$ in the objective function given by (12) is used instead of the decision variable $|\Delta P_g^G|$ in the objective function given by (6).

## IV. Solution Procedure

There is a variety of solution methods reported in the literature for bilevel optimization problems. These are mainly constructed based upon a conversion into the equivalent single-level models, using optimality Karush–Kuhn–Tucker conditions and duality theory [31]. We present functions $f$ and $h$ by applying graph theory and breadth-first search (BFS) algorithm described in [32]. Therefore, the optimization problem (1)–(5) cannot be converted to an equivalent single-level optimization.

In this study, GA-based method is used to solve two optimization problems given by (1)–(11) and (1)–(5), (12)–(19). The following sections provide a detailed description of the solution algorithm. It should be noted that any other metaheuristic algorithm could be employed similarly.

### *A. Solving the Upper Level Problem*

Two optimization problems (1)–(11) and (1)–(5), (12)–(19) can be formulated as given in the following:

$$\max_{\overline{Z}^L} \sum_{d \in \Omega_D} LS_d^D \tag{20}$$

subject to: (2)–(5) and

$$\overline{LS}^D = S(\overline{Z}^L, \overline{W}^G(\overline{Z}^L), \overline{W}^D(\overline{Z}^L)) = U(\overline{Z}^L) \tag{21}$$

where the last constraint describes the lower level problem. The function within arg{*} in (6) or (12) is formulated as functions "$S$" and "$U$".

The solution algorithm is shown in Fig. 2. Any individual in the population of each GA generation makes a possible suggestion for $\overline{Z}^L$. Given this value of $\overline{Z}^L$, the vectors $\overline{W}^G(\overline{Z}^L)$ and $\overline{W}^D(\overline{Z}^L)$ are determined by developing the subprogram of evaluating communication links and specifying the disconnected buses based on graph theory and BFS algorithm. For the specified values of $\overline{Z}^L$, $\overline{W}^G$, and $\overline{W}^D$, the solution of the lower level problem (according to OSE A/B) is invoked in an LP/MILP solver (e.g., CPLEX from GAMS). The results of this step are returned to GA to identify the fitness of each individual of the population ($LS_d^D$ value). Next, GA operators (selection, crossover, and mutation) are used to produce the next generation. This procedure is repeated to satisfy the stopping criterion.

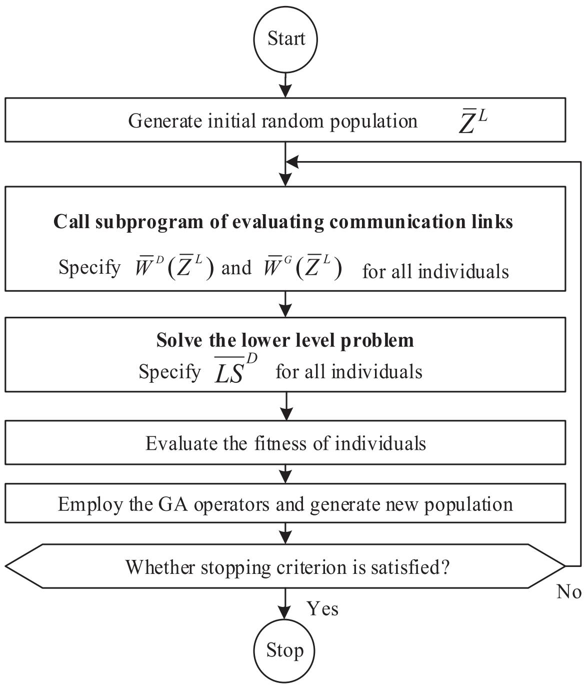
Start
Generate initial random population $\overline{Z}^L$
Call subprogram of evaluating communication links
Specify $\overline{W}^D(\overline{Z}^L)$ and $\overline{W}^G(\overline{Z}^L)$ for all individuals
Solve the lower level problem
Specify $\overline{LS}^D$ for all individuals
Evaluate the fitness of individuals
Employ the GA operators and generate new population
Whether stopping criterion is satisfied?
No
Yes
Stop

Fig. 2. Flowchart of the solution procedure.

### *B. Solving the Lower Level Problem*

*OSE A*: By using the linear expression of $|\Delta P_g^G|$ in (6)–(11), an LP problem can be obtained. Equation (22) is applied to linearize $|\Delta P_g^G|$. Thus, the value of $\Delta P_g^G$ is described as (23)

$$|\Delta P_g^G| = \Delta P_g^{G+} + \Delta P_g^{G-} \tag{22}$$

$$\Delta P_g^G = \Delta P_g^{G+} - \Delta P_g^{G-}. \tag{23}$$

In (22) and (23), $\Delta P_g^{G+}$ and $\Delta P_g^{G-}$ are defined as the positive variables. Then, constraint (9) is substituted by (24) and (25) that completes the linearization scheme

$$0 \leq \Delta P_g^{G+} \leq P_{g,\mathrm{inc}}^G - P_g^G \quad \forall g \in \Omega_G \tag{24}$$

$$0 \leq \Delta P_g^{G-} \leq P_g^G - P_{g,\mathrm{dec}}^G \quad \forall g \in \Omega_G. \tag{25}$$

*OSE B*: The model (12)–(19) is an MILP problem.

## V. Numerical Results

The proposed model is implemented in 24-bus IEEE reliability test system (RTS) [33]. This system contains 32 generation units, 17 loads, and 38 transmission lines. The system's peak demand is 2850 MW and further information is given by [33]. The system also contains four parallel lines that an attacker requires to individually allocate necessary resources on them. Besides, to select these lines, the allocated resources must be twice as of those required for one attack. Moreover, the minimum output power of all generation units is zero.

The algorithm presented in Fig. 2 is implemented by employing both MATLAB and GAMS so that GA is run in MATLAB and the lower level problems are solved in GAMS. Our proposed model is implemented by using a laptop with the Core i5 2.67-GHz processor and 4-GB RAM. Several case studies are

TABLE I
COMPARISON OF CASE STUDIES

| Case study | Coefficients $\alpha$ and $\beta$ | OSE | The location of control center | Loading level |
|---|---|---|---|---|
| 1st | Variable | OSE A | Bus 11 | 100% |
| 2nd | 10 000 | OSEs A and B | Bus 11 | 100% |
| 3rd | Variable | OSE A | Buses 11 and 16 | 100% |
| 4th | 10 000 | OSE A | Buses 11 and16 | 80%,100% |

TABLE II
RESULTS OF VULNERABILITY ANALYSIS IN THE FIRST CASE, ($R = 2{,}4$)

| | | $R = 2$ | | $R = 4$ | |
|---|---|---|---|---|---|
| $\alpha$ | $\beta$ | Load shedding (MW) | Attacked transmission lines | Load shedding (MW) | Attacked transmission lines |
| 10 | 100 | 459 | 19, 30 | 876 | 11, 15, 19, 30 |
| 20 | 200 | 836.7 | 23, 30 | 1051.9 | 1, 11, 23, 30 |
| 30 | 300 | 836.7 | 23, 30 | 1094 | 9, 11, 23, 30 |
| 100 | 1000 | 836.7 | 23, 30 | 1094 | 9, 11, 23, 30 |
| 1000 | 10 000 | 836.7 | 23, 30 | 1184.6 | 5, 11, 16, 17 |
| 10 | 10 | 194 | 19, 23 | 567 | 18, 25, 26, 28 |
| 20 | 20 | 194 | 19, 23 | 587.9 | 6, 14, 15, 16 |
| 100 | 100 | 459 | 19, 30 | 992.3 | 5, 11, 16, 17 |
| 10 000 | 10 000 | 836.7 | 23, 30 | 1199.3 | 12, 15, 16, 17 |

designed, which are introduced in Table I. In each case study, impacts of changes in several practical parameters are studied which are separately described in the following sections.

The standard weighting coefficients in a real power system are determined by employing a heuristic method. Considering the descriptions in Section III-B, the coefficient $\alpha$ is selected within a given range (e.g., 10–1000) and $\beta$ is set equal to tenfold $\alpha$ to model the further delay in generation units' response. In some cases, $\alpha$ and $\beta$ are set identical and equal to a value greater than the maximum load (in MW) such that the SO tries to minimize load shedding through the communication-connected buses and otherwise minimizes the load shedding and also changes of generation units' production by using communication-disconnected buses.

### A. *First Case Study: The Impacts of Delay in Response*

The impact of changes in coefficients $\alpha$ and $\beta$ within the objective function is studied in this section that potentially clarifies the impacts of the delay in response. The communication network is not included in the original version of RTS and thus the required topology is established through solving a shortest-path LP problem presented in [34].

The numerical results are shown in Table II. In the first case, the value of coefficient $\beta$ is kept greater than that of $\alpha$, as given in top of Table II. These two values are considered in this way to increase the delay in generation units' response compared to that of load buses [28], [29]. As can be seen in Table II, the value of the weighting coefficients affects the attacked transmissions lines and also the amount of load to be shed. For instance, the first and fifth rows of Table II for $R = 4$ show that by increasing the weighting coefficients 100-fold, the attack scenario is completely changed and the amount of load shedding is also increased up to 35% approximately. Thus, the more delays in response of communication-disconnected generation units in comparison to that of communication-disconnected load buses would lead to the more damage to the network. This happens since the attacker takes disruptive actions knowing that how the SO as well as other system components would respond to the communication paths failures. In this way, the attacker attempts to damage those lines that would lead the SO to rather shed more load than to adjust the generation units' production.

The coefficients $\alpha$ and $\beta$ are considered equal in bottom of Table II. For the greater values of these coefficients, the communication-disconnected components may have a greater delay in response to the emergency situations that may require the connected load buses to shed larger loads to retain the entire network in a balanced condition.

To better understand the model performance, consider the eighth row of Table II that corresponds to $R = 2$ with $\alpha, \beta = 100$. Once the lines 19 and 30 run out of service, it will require a load shedding equal to 459 MW, whereas given the last row ($\alpha, \beta = 10\ 000$), 836.7 MW of load might be shed in case of an attack on line 23 instead of 19. If line 19 is attacked in latter, the required load shedding would be equal to 831.7 MW, that is 5 MW less than the reported value. In brief, when applying different delay scenarios by changing the weighting coefficients, the attacker may have a different range of transmission line targets to maximize damage in the system. Thus, when an alternative communication infrastructure with a higher data rate is provided, it prevents more damage.

As seen in the fifth and eighth rows of Table II, the attack scenarios for $R = 4$ are the same, but they differ in the amount of load to be shed. Indeed, with the failure of the same lines, the greater delay in response of communication-disconnected generation units (when $\beta = 100$ in comparison with $\beta = 10$) requires the SO to shed more loads of the communication-connected load buses (at a lower cost of the objective function) to preserve the system balanced.

### B. *Second Case Study: The Impacts of Considering OSEs (Justifying the Proposed Model)*

To justify our proposed model, a detailed comparison between our model and the model proposed in [9] is discussed in this case study. Table III presents the comparison results.

In all studies, when taking the impact of communication paths into account, the greater amounts of load shedding are required. This underlines that when the communication paths between the SO and different components of the system are failed (resulting in delayed responses), the greater amounts of load shedding are required to keep the power system balanced. Given the row of $R = 4$ in Table III, transmission lines 7, 21, 22, and 23 are attacked according to the model of [9], whereas considering the communication network along with the OSE, those lines are changed to 12, 15, 16 and 17 and 5, 11, 16 and 17 as specified by OSE A and B, respectively. This may also cause wider damage inflicted on the power system. These cases demonstrate that neglecting the impact of communication network disconnection may result in large inaccuracy and error in analyzing

TABLE III
IMPACTS OF CONSIDERING OSES A AND B IN THE VULNERABILITY ANALYSIS MODEL PROPOSED IN [9]

| | Considering OSE A | | | Considering OSE B | | | Model of [9] | |
|---|---|---|---|---|---|---|---|---|
| $R$ | Load shedding (MW) | Attacked transmission lines | Rate of increase (%) compared to the results of [9] | Load shedding (MW) | Attacked transmission lines | Rate of increase (%) compared to the results of [9] | Load shedding (MW) | Attacked transmission lines |
| 2 | 836.7 | 23,30 | 331% | 194 | 19,23 | 0% | 194 | 19,23 |
| 4 | 1199.3 | 12,15,16,17 | 132% | 1309.6 | 5,11,16,17 | 154% | 516 | 7,21,22,23 |
| 6 | 1406 | 5,8,11,12,16,28 | 38% | 1536 | 9,11,19,30,32,33 | 51% | 1017 | 7,11,15,17,18,23 |
| 8 | 1450 | 1,2,3,11,<br>12,15,16,34 | 21% | 1640 | 3,11,18,21,<br>22,25,26,28 | 37% | 1198 | 15,17,18,25,<br>26,28,36,37 |
| 10 | 1482 | 3,11,18,21,22,<br>25,26,28,36,37 | 8% | 1940 | 11,16,18,21,22,<br>25,26,28,30,38 | 41% | 1373 | 11,15,17,18,25,<br>26,28,36,37 |

the power system's vulnerability. Furthermore, the OSE is also very important in this problem.

Additionally, as seen in Table III, when $R$ increases, the rate of increase in load shedding compared to that of the last column decreases. This is because of the fact that a proportion of total demand for the power system, that is 2850 MW, is well supplied by the local generation units connected to corresponding load buses. Hence, as the number of attacks increases, the rate of increase of the load shedding decreases. Unlike this, when meeting less attacks (i.e., particularly $R = 2$ and 4), the results vary considerably as obviously indicated by the extensive damage when considering different OSEs.

A detailed comparison of two proposed OSEs shows that the required load shedding in OSE B is greater than that of OSE A. The instance is within all studies except when $R = 2$. This is due to a constraint applied on the communication-disconnected generation units when responding in emergency situations. OSE B mandates that communication-disconnected generation units must either stay in operation at the previous operating point or be shut down. Moreover, at a generation unit shutdown scenario, it may lead to further imbalance between the load and generation and thus more load shedding.

## *C. Third Case Study: The Impacts of Control Center's Location*

The location of the control center likely affects the interdependence of the power system and communication network, which is investigated in this case study. Bus 16 is selected as another location of the control center. The corresponding communication network scheme is obtained through the shortest-path method [34]. Bus 16 is selected to fulfill the purpose of choosing buses located on the network edge (instead of bus 11 that is located on the center). Table IV compares different amounts of load shedding for a range of $R$, $\alpha$, and $\beta$ values. As can be observed, the damage to the power system and also the attack scenario are strongly affected by the location of control center. Moreover, the results associated with two different locations do not follow a fixed trend. They are also affected by the factors such as weighting coefficients $\alpha$ and $\beta$ and resource limitation $R$. However, investigating the optimal location of the control center to minimize the vulnerability is beyond the scope of this paper and is currently an ongoing research.

In analyzing the results of more attacks (i.e., $R = 8$ and 10), it is observed that in case of locating the control center in the geographic center of the network (bus 11), less amounts of loads are required to be shed than that of required when the control center is placed on the network edge (bus 16). Indeed, locating the control center in the center of the power system can lead to less communication-disconnected components at the postattack time, since the number of transmission lines on which the attacks lead to large number of communication-disconnected components could be reduced. In turn, this issue would be accentuated in case of large-scale power systems, in which more resources are required to inflict damage.

## *D. Fourth Case Study: The Impacts of Power System Loading*

The corresponding results are provided in Table V. It is observed that while reducing loading level of the network, the amount of load to be shed is reduced for identical number of attacks, as expected. However, the attacked lines have notably been changed. Therefore, it is concluded that while considering the communication network impact and also the delay in components' response, the total amounts of system load shedding are affected by the system operating point and also its loading.

The results indicate that as the system loading reduces, the percentage of load shedding affected by PDAs also decreases. More precisely, as the power system is operated in a more stressed operating point, it is more likely to be more vulnerable. Thus, the best time to attack the power system is when the system is operated at its peak load point or near that. This is due to the fact that in the case of peak loading, the SO is less flexible to appropriately respond and restore the system to normal conditions.

It should be noted that in some cases, the amounts of load shedding are close in magnitude when even the number of attacks has increased. As an example, in case of 80% loading of the peak value, changing $R$ from six to eight results in only 0.1 MW increase in the required load to be shed.

## *E. Computational Issues*

Generally, the following four different factors affect the run time.

1) *Setting GA Parameters:* The most important factors affecting the run time include the GA parameters such as the

TABLE IV
COMPARISON OF VULNERABILITY IN THE TWO PROPOSED COMMUNICATION NETWORK PLANS CONSIDERING OSE A

| *R* | $\alpha, \beta$ | Bus 11 as control center | | Bus 16 as control center | |
|---|---|---|---|---|---|
| | | Load shedding (MW) | Attacked transmission lines | Load shedding (MW) | Attacked transmission lines |
| 2 | 10 | 194 | 19, 23 | 232.4 | 23, 29 |
| | 100 | 459 | 19, 30 | 232.4 | 23, 29 |
| | 10 000 | 836.7 | 23, 30 | 232.4 | 23, 29 |
| 4 | 10 | 567 | 18, 25, 26, 28 | 931 | 7, 21, 22, 23 |
| | 100 | 992.3 | 5, 11, 16, 17 | 931 | 7, 21, 22, 23 |
| | 10 000 | 1199.3 | 12, 15, 16, 17 | 1218 | 11, 16, 17, 28 |
| 6 | 10 | 1046 | 11, 18, 21, 22, 23, 27 | 1046 | 3, 11, 21, 22, 23, 27 |
| | 100 | 1144.4 | 5, 8, 11, 12, 16, 28 | 1065.7 | 21, 22, 23, 24, 25, 26 |
| | 10 000 | 1406 | 5, 8, 11, 12, 16, 29 | 1314.3 | 11, 12, 13, 15, 16, 17 |
| 8 | 10 | 1208 | 11, 18, 21, 22, 23, 24, 25, 26 | 1228 | 3, 11, 21, 22, 23, 24, 25, 26 |
| | 100 | 1251 | 6, 8, 11, 14, 15, 16, 31, 38 | 1280 | 7, 20, 21, 22, 23, 29, 36, 37 |
| | 10 000 | 1450 | 1, 2, 3, 11, 12, 15, 16, 38 | 1508.2 | 3, 17, 24, 25, 26, 31, 32, 33 |
| 10 | 10 | 1435 | 3, 7, 11, 18, 21, 22, 23, 29, 36, 37 | 1453 | 11, 15, 17, 18, 23, 25, 26, 28, 36, 37 |
| | 100 | 1482 | 3, 11, 18, 21, 22, 25, 26, 28, 36, 37 | 1482 | 9, 11, 18, 21, 22, 25, 26, 28, 36, 37 |
| | 10 000 | 1482 | 3, 11, 18, 21, 22, 25, 26, 28, 36, 37 | 1551.7 | 1, 11, 13, 14, 15, 17, 18, 22, 36, 37 |

TABLE V
COMPARISON OF VULNERABILITY UNDER PEAK LOAD AND 80% OF PEAK LOAD CONDITIONS

| | Peak load conditions (bus 11 as control center) | | | 80% of peak load condition (bus 11 as control center) | | |
|---|---|---|---|---|---|---|
| *R* | Load shedding (MW) | Attacked transmission lines | $\mathrm{MW/MW_{peak}}$ | Load shedding (MW) | Attacked transmission lines | $\mathrm{MW/MW_{peak}}$ |
| 2 | 836.7 | 23, 30 | 0.29 | 564 | 19, 30 | 0.25 |
| 4 | 1199.3 | 12, 15, 16, 17 | 0.42 | 874.4 | 11, 13, 16, 17 | 0.38 |
| 6 | 1406 | 5, 8, 11, 12, 16, 29 | 0.49 | 961.7 | 6, 11, 13, 15, 16, 17 | 0.42 |
| 8 | 1450 | 1, 2, 3, 11, 12, 15, 16, 38 | 0.51 | 961.8 | 6, 11, 13, 15, 16, 17, 25, 26 | 0.42 |
| 10 | 1482 | 3, 11, 18, 21, 22, 25, 26, 28, 36, 37 | 0.52 | 1109 | 4, 5, 11, 15, 16, 17, 18, 29, 36, 37 | 0.49 |

TABLE VI
GA PARAMETERS

| Population size | Iterations | Selection probability | Crossover probability |
|---|---|---|---|
| 30 | 500 | 0.2 | 0.1 |

TABLE VII
RUN TIME FOR THE FIRST CASE STUDY

| *R* | 2 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|
| Run Time (s) | 1443 | 1788 | 2209 | 2722 | 2925 |

initial population, number of iterations, selection probability, and mutation probability. According to the GA performance, as much as the initial population and the iterations are larger, more time will be needed to solve it. The adjustment of these parameters depends on the length of the decision variable vector as well as the type of the GA operators. The GA parameters chosen here are given in Table VI.

2) *The Maximum Number of Targeted Lines (R):* In the GA, each chromosome of any given generation contains a vector of transmission lines as candidates for the PDA. To impose the limitation on the maximum amounts of the attacker's resources which is given by (2), GA uses the penalty method for the chromosomes that violate the constraint. Therefore, for greater values of $R$, it is less likely that a chromosome violates the constraint, and thus more scenarios should be sent to the lower level problem to determine their objective functions value. Consequently, the simulation would take more time.

3) *Information Exchange Between Upper and Lower Level Problems:* The attack scenario (the binary vector $\overline{Z}^L$) is reported from MATLAB into GAMS as the input of the lower level problem, and in reverse, the value of the resulted objective function (a real number) is returned to the upper level problem. The data are exchanged over a very short period of time.

4) *Lower Level Subprogram in GAMS:* Given that the lower level problem is the LP or MILP one, it is solved easily. However, it might take longer time to reach the solution in MILP.

To estimate the computational burden of the model in the RTS, the run time is reported for the first case study in Table VII. The parameters reported in Table I are the perfect choice for solving the proposed model based on RTS. Generally, as the size of the test system is larger (including more transmission lines as candidates for the attack), the greater initial population to add variety to the solutions and the more extensive search throughout the feasible solution space, as well as more iterations to conduct a more accurate search, would be needed. However, because the computation is done in an offline process and also reaching the solution in a short period of time is not a high priority, it is expected that the proposed model would enjoy an appropriate performance when studying even a real-sized power systems.

## VI. Conclusion and Further Works

This paper proposes a new bilevel optimization-based model to evaluate the vulnerability of a power system, which is geographic-cyber interdependent with communication network. This paper is remarkable due to the fact that it models simultaneous PDAs on the power system and communication network, while considering the impacts of communication network disruption on the corrective actions taken by the power SO. Numerical results show that the vulnerability of a power system under PDAs likely increases when considering the geographic-cyber interdependence. Further, the simulations reveal the profound impact of power system operation strategies in emergency to minimize the damage caused by PDAs. They also demonstrate that the power control center's location and thus the topology of the communication network might, in fact, lessen the damage. Therefore, operation instructions and the communication network infrastructure should be designed in such a way that the vulnerability of a power system due to PDAs is mitigated.

As the first attempt to study geographic-cyber interdependence of the power system and communication network, the fiber-optic network is the only main communications infrastructure that was considered. Moreover, we took into account a simplified power system operation model (in normal and emergency conditions). The future work is intended to extend this model to consider the other communication infrastructures and reactive power study.

## References

[1] European Commission. (2006, Dec. 12). *European Program for Critical Infrastructure Protection*. [Online]. Available: https://ec.europa.eu/home-affairs/what-wedo/policies/crisis-and-terrorism/critical-infrastructure

[2] U.S. Dep. Homeland Security. (Dec. 2013), *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. [Online]. Available: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[3] X. Yu and Y. Xue, "Smart grids: A cyber-physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016, doi: 10.1109/JPROC.2015.2503119.

[4] G. Brown, M. Carlyle, J. Salmeron, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, Nov. 2006, doi: 10.1287/INTE.1060.0252.

[5] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Syst. Mag.*, vol. 21, no. 6, pp. 11–25, Dec. 2001, doi: 10.1109/37.969131.

[6] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012, doi: 10.1109/TSG.2012.2194520.

[7] "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," U.S.–Canada Power Syst. Outage Task Force, Office Electr. Del. and Energy Reliab., U.S. Dept. Energy, Washington, DC, USA, Tech. Rep., Apr. 2004.

[8] *PJM Manual 01: Control Center and Data Exchange Requirement*, Nov. 2014.

[9] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Gener. Transmiss. Distrib.*, vol. 4, no. 2, pp. 178–190, Feb. 2010, doi: 10.1049/IET-GTD.2009.0098.

[10] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Syst. J.*, vol. 6, no. 3, pp. 481–487, Sep. 2012, doi: 10.1109/JSYST.2012.2190688.

[11] E. I. Bilis, W. Krger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Syst. J.*, vol. 7, no. 4, pp. 854–865, Dec. 2013, doi: 10.1109/JSYST.2012.2223512.

[12] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004, doi: 10.1109/TPWRS.2004.825888.

[13] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat," *IEEE Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005, doi: 10.1109/TPWRS.2005.851942.

[14] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005, doi: 10.1109/TPWRS.2005.846198.

[15] A. 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, doi: 10.1109/TPWRS.2006.889080.

[16] L. Zhao and B. Zeng, "Vulnerability analysis of power grids with line switching," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2727–2736, Aug. 2013, doi: 10.1109/TPWRS.2013.2256374.

[17] S. Sayyadipour, G. R. Yousefi, and M. A. Latify, "Mid-term vulnerability analysis of power systems under intentional attacks," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 15, pp. 3745–3755, Aug. 2016, doi: 10.1049/IET-GTD.2016.0052.

[18] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014, doi: 10.1109/TSG.2014.2310742.

[19] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016, doi: 10.1109/TSG.2015.2456107.

[20] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011, doi: 10.1109/TSG.2011.2123925.

[21] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 104–111, Feb. 2015, doi: 10.1109/TII.2014.2367322.

[22] K. R. Davis *et al.*, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015, doi: 10.1109/TSG.2015.2424155.

[23] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013, doi: 10.1109/TSG.2012.2232318.

[24] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015, doi: 10.1109/TSG.2014.2372315.

[25] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 3–13, Jan. 2014, doi: 10.1109/TSG.2013.2280399.

[26] *IGMC Manual in Permanent Instructions of Operation: Operation Instructions in Case of Communication Loss*. Dec. 2012. [Online]. Available: http://www.igmc.ir

[27] *PJM Manual 12: Balancing Operations*, Apr. 2015.

[28] *PJM Manual 14D: Generator Operational Requirements*, May 2015.

[29] *IGMC Manual in Permanent Instructions of Operation: Frequency Control*. Dec. 2012. [Online]. Available: http://www.igmc.ir

[30] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, *Power Generation, Operation and Control*, 3rd ed. Hoboken, NJ, USA: Wiley, 2013.

[31] S. Dempe, *Foundations of Bilevel Programming*. Norwell, MA, USA: Kluwer, 2002.

[32] T. H. Cormen and C. E. Leiserson, *Introduction to Algorithms*. Cambridge, MA, USA: MIT Press, 2009.

[33] 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, doi: 10.1109/59.780914.

[34] G. Sierksma and D. Ghosh, *Networks in Action: Text and Computer Exercises in Network Optimization*. New York, NY, USA: Springer, 2009.

Authors' photographs and biographies not available at the time of publication.