energies

MDPI

Article

Optimal Deception Strategies in Power System Fortification against Deliberate Attacks

Peng Jiang [1,2], Shengjun Huang [1,*] and Tao Zhang [1,3]

1 College of Systems Engineering, National University of Defense Technology, Changsha 410073, China; jiangpeng_nudt@aliyun.com (P.J.); zhangtao@nudt.edu.cn (T.Z.)
2 Energy Internet Research Center, China Aerospace Science and Technology Corporation, Beijing 100048, China
3 State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, China
* Correspondence: huangshengjun@nudt.edu.cn; Tel.: +86-152-0080-9007

Received: 27 December 2018; Accepted: 17 January 2019; Published: 22 January 2019

Abstract: As a critical infrastructure, the modern electrical network is faced with various types of threats, such as accidental natural disaster attacks and deliberate artificial attacks, thus the power system fortification has attracted great concerns in the community of academic, industry, and military. Nevertheless, the attacker is commonly assumed to be capable of accessing all information in the literature (e.g., network configuration and defensive plan are explicitly provided to the attacker), which might always be the truth since the grid data access permission is usually restricted. In this paper, the information asymmetry between defender and attacker is investigated, leading to an optimal deception strategy problem for power system fortification. Both the proposed deception and traditional protection strategies are formulated as a tri-level mixed-integer linear programming (MILP) problem and solved via two-stage robust optimization (RO) framework and the column-and-constraint generation (CCG) algorithm. Comprehensive case studies on the 6-bus system and IEEE 57-bus system are implemented to reveal the difference between these two strategies and identify the significance of information deception. Numerical results indicate that deception strategy is superior to protection strategy. In addition, detailed discussions on the performance evaluation and convergence analysis are presented as well.

Keywords: two-stage robust optimization; power system fortification; deception strategies; column-and-constraint generation; information asymmetry

1. Introduction

In order to facilitate the community to achieve stable and reliable power supply, a lot of new technologies and equipment are extensively integrated into the modern power grid, such as advanced metering infrastructure (AMI) and intelligent electronic device (IED). Definitely, the integration of new items complicates the network, leading to a reduction of system invulnerability since more accessories mean higher failure probability and the supervisory control and data acquisition (SCADA) is more difficult to implement in complex systems [1]. In addition to critical reliability issues, the power grid suffers various types of threats, e.g., accidental natural disaster attacks [2,3] and deliberate artificial attacks (military or terrorist, since power grid is a critical infrastructure) [4], causing huge economic losses and major social impacts due to the resulting cascading failures. Therefore, the power system fortification has attracted great concerns in the community of academics, industry, and military.

In order to design a robust fortification plan, the target attack pattern should be determined first. It is reported in [5] that attacks are mainly implemented on three aspects: physical, cyber, and human

since the power grid is a cyber-physical interconnected network operated by engineers. For quick reference, Figure 1 depicts a full scheme of different attacks, where each type is investigated in the literature with either separated or coordinated pattern. In [6], a general mathematical framework for cyber-physical systems, attacks, and monitors is proposed for power systems, transportation networks, industrial control processes, and critical infrastructures. In [7], several physical attack scenarios are fabricated and investigated, where system potential cascading events are modeled with power flow calculation, hidden failures are simulated by the Monte Carlo method, and operator performance is analyzed via a simple human reliability model. Cyber systems are extensively integrated in the physical grid for power generation, transmission, and distribution, such as communication networks, metering units, and control centers, etc. [8]. In cyber-physical systems, deliberate attacks are implemented not only on their physical infrastructure, but also on their data management and communication layer [6]. A comprehensive review of false data injection attack (FDIA) is given in [9], where theoretical basis, physical and economical impacts, defensive strategies, and potential future research directions of FDIA are investigated and discussed. The optimal attacks implemented on substations and transmission lines are investigated in [10] based on the proposed component interdependency graph. The contribution and impact of branches when they are employed or removed from a power system are analyzed in [11], leading to the identification of sensitive regions of each line based on a cyclic addition algorithm. In Refs. [12] and [13], the cascading failures caused by line breakdown is investigated using complex network theories, such as small-world and scale-free networks, where electrical characteristics of nodes are considered on the basis of pure structure topology. Although there are various types of attacks, physical attack via tripping lines is determined as the target attack pattern in this paper. We intend to claim that, although the exemplified attack is tripping lines, the solution methodology reported in this paper can be easily extended to other types of attacks.

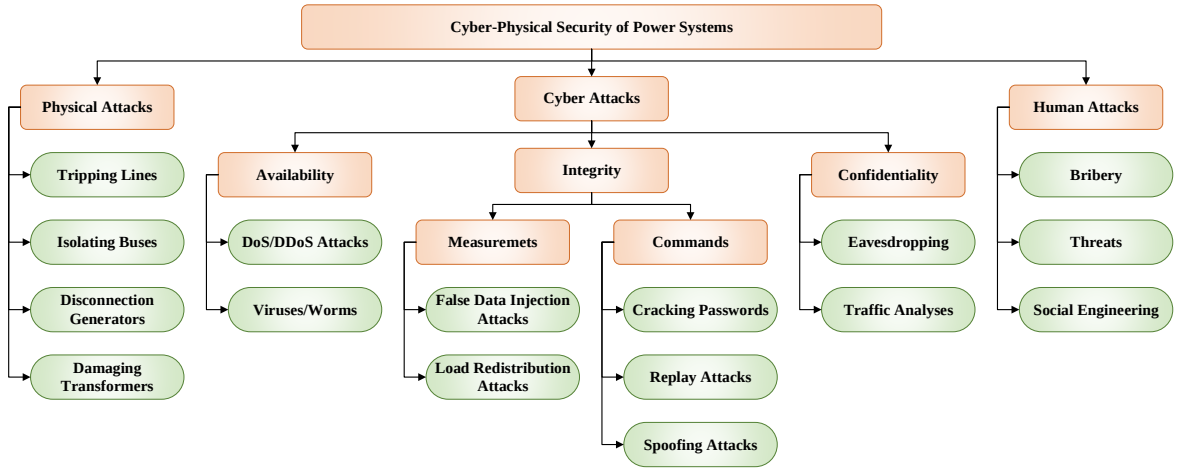


Figure 1. Various types of attacks against the modern power grid [5].

Faced with different kinds of attacks, the defensive plan could be various. Taking the tripping line attack as an example, the defensive strategy includes: (1) adding new devices (both generators and transmission lines) to improve the redundancy; (2) enhancing the defensive strength to guarantee the protected assets are invulnerable during attacks; and (3) allocating portable components (e.g., distributed generators) to dynamically reconfigure the distribution network. Whatever the attack pattern and defense resource are, the optimization problem of generating an optimal defensive plan is related to two opposite agents, i.e., the defender and attacker to protect and destroy the system respectively. According to the number of action rounds, the game between these agents can be classified as an attacker–defender (AD) model and the defender–attacker–defender (DAD) model. Traditionally, the AD model is formulated as the bi-level min–max programming problem, which is challenging due to its non-convex discrete property. In [14], an equivalent single-level reformulation of the AD model

is proposed to address the optimal defense problem, where transmission line switching is employed for protection. A coordinated cyber-physical attack is analyzed in a proposed bi-level model in [15], which is transformed into a mixed-integer linear programming (MILP) problem and addressed via a rigorous two-stage solution approach. In order to investigate cyber-attack on multiple transmission lines in economic dispatch, a bi-level MILP model with the capability to overload branches is proposed in [16], where remarkable computational efficiency is achieved.

On the other hand, the DAD model is usually formulated as a tri-level programming problem with three rounds of action [17]:

- In the first stage (upper-level problem), the defender determines an optimal defensive plan with the goal of minimizing system power imbalance/mismatch, where the reaction of attacker should be considered and the defensive resource is limited.
- In the second stage (middle-level problem), the attacker is faced with an enhanced system where the defensive plan generated in the first stage has been implemented, and whose goal is maximizing the unserved energy of the confronted network with restricted attack resources.
- In the third stage (lower-level problem), both initial defensive plan and subsequent attack scheme have been carried out, leading to a partially destroyed system, whose power imbalance will be minimized in this stage via system redispatch.

In order to defend against terrorist attacks, a tri-level optimization model of resource allocation is proposed in [18], which is then tackled by a decomposition approach. The superiority of tri-level optimization over bi-level optimization in electric power network defense is validated with case studies. In [19], uncertain attacks and load types are integrated into the DAD model for power system protection, which is then addressed by two-stage robust optimization (RO) approach and column-and-constraint generation (CCG) algorithm. The CCG method is proposed in [20] and [21], whose performance in RO framework has been extensively verified on different types of power system optimization problems, such as transmission expansion planning [22], economic dispatch [23], unit commitment [24], and distribution network reconfiguration [25], etc. Based on RO and CCG, a lot of power system defensive research has been implemented, e.g., Ref. [26] investigates the problem of allocating fortification resources with the objective of maximizing the power system's immunity against malicious attacks, Ref. [27] proposes an approach to mitigate network vulnerability toward worst-case spatially localized attacks, and Ref. [28] develops a practical and efficient tool for utility transmission planners to protect critical facilities from potential physical attacks, etc.

Although advanced algorithms and sophisticated problem formulations are proposed in the literature, one limitation is shared in the above references, i.e., the attacker is assumed to be capable of accessing sufficient information. The attacker's decision is made in the second stage based on all information revealed at that time. In the literature, it is commonly assumed that all information is accessible by the attacker including network topology, device parameters, physical capacity, and defensive decisions made by the defender in the first stage. Nevertheless, it is very difficult or even impossible to get access all information, especially in war and terrorist attacks where the defender is supposed to hide some critical information or even do some deception activities. Actually, in a DAD model, the attacker is exposed to the defender due to: (1) the attacker always intends to cause the worst consequence, thus the decision can be figured out if the input information is fixed; and (2) the defender's decision can withstand the worst case incurred by the attacker, not to mention those randomly generated attack plans. It can be concluded that there is an information asymmetry between the defender and attacker, which can be utilized to squeeze benefits. For example, given a real configuration A, if the information is symmetry, then the worst attack plan B will be proposed by the attacker, leading to a system power imbalance M. On the other hand, if the deception strategy is implemented to show a fake configuration A' to the attacker, then the worst attack plan B' will be generated, whose power mismatch is M'. For real configuration A, as the DAD model is targeted at

the worst case, it can be concluded that there is no attack can produce larger power mismatch than M, i.e., $M' \leq M$, thus the system power imbalance might be reduced by information asymmetry.

In this paper, we intend to investigate the optimal deception strategies in power system fortification against deliberate attacks. The deception strategy is described in detail based on a full comparison with the traditional protection strategy in Section 2. According to the step-by-step theoretical analysis of a 6-bus system, the potential of deception strategy is revealed. In order to numerically derive the optimal deception and protection strategy, tri-level programming problems are established based on the DAD model. In accordance with the literature, the tri-level programming problem is addressed with RO in Section 3, where both subproblem and master problem are explicitly formulated based on dual theory, big-M method, and CCG constraints. Case studies are implemented on a 6-bus system and the IEEE 57-bus system in Section 4, where the smaller network is utilized to identify the superiority and analyze the inner mechanism, while the larger system is employed to investigate the performance under different circumstance and discuss the convergence property. Results indicate that the deception strategy achieves less unserved power and faster convergence rate. Finally, conclusions and future work are summarized in Section 5.

The main contributions of this paper are as follows: (1) the deception conception is proposed and formulated, providing a general framework for more complicated defensive strategies based on information asymmetry in the future; (2) an RO solution framework for the optimal deception strategy is developed on the basis of CCG constraints, and the convergence property is discussed; and (3) comprehensive numerical experiments are implemented to verify the advantageous of deception strategy, including less objective value and faster convergence rate.

2. Problem Formulation

In this section, the target problem will be established based on the illustrative description and mathematical formulation. In Section 2.1, the deception and protection strategies in power system fortification are illustrated, compared, and discussed based on an invented 6-bus power system. Section 2.2 gives a tri-level MILP formulation for the deception strategy, based on which the optimal protection problem is derived as well. The abbreviation and nomenclature are attached at the end of this paper.

2.1. Differences between Deception and Protection Strategies

In order to establish the significance of this work, the deception strategy is compared with conventional protection program in this subsection. A 6-bus system with eight branches shown in Figures 2a and 3a is employed for demonstration, where nodes 1 and 2 are generators. For the sake of fairness and justice, it is assumed that both strategies have the same candidate set and implementation capability. In this example, all existing branches can be deceived/protected, and the maximum number of lines to be hidden/enhanced is 2 due to the limited budget.

Figure 2 depicts the deception strategy in power system fortification. If branches 1–5 and 2–4 are hidden, the resulted power system shown in Figure 2c will be presented to the adversary. Given an attack budget (in this example, it is assumed that the budget can be utilized for tripping branch is 2), the attacker can easily derive an attack plan as shown in Figure 2d by the solution of a bilinear *max-min* problem to isolate all four load buses. Figure 2e displays the expected power system by the terrorist after attack, which is obtained from Figure 2c by the elimination of Figure 2d. Nevertheless, the actual power system after attack should be Figure 2f, which is retrieved from Figure 2a by the excluding of Figure 2d. It should be pointed out that the resulted system would be Figure 2e if no deception strategy is adopted, whose load curtailment is very large since two generators are isolated. On the other hand, the unserved energy in Figure 2f could be as low as 0 since all loads are connected to the generator. It is worth noting that the observed (target) systems for defender and attacker are different, i.e., Figure 2a,c respectively; therefore, the deliberate attack plan proposed by the attacker

based on Figure 2c has a limited impact over Figure 2a. The difference between defender and attacker on the observed system is defined as information asymmetry in this paper.

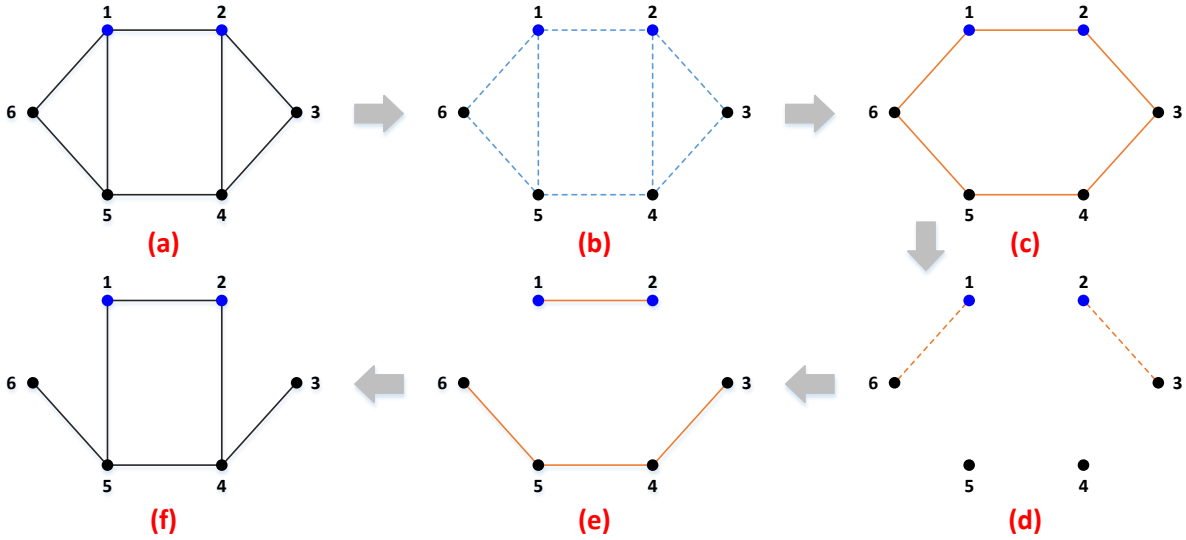


Figure 2. Demonstration of deception strategies in power system fortification: (**a**) original power system; (**b**) candidate deception branch set; (**c**) deceived power system shown to the adversary; (**d**) deliberate attack plan; (**e**) expected power system by the terrorist after attack; (**f**) actual power system after attack.

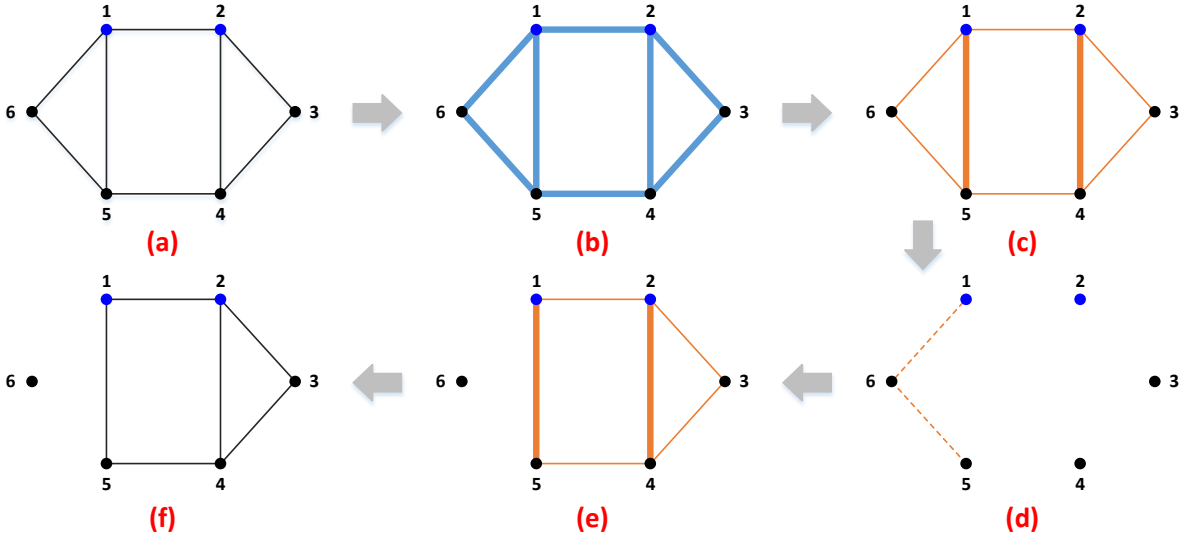


Figure 3. Demonstration of protection strategies in power system fortification: (**a**) original power system; (**b**) candidate protection branch set; (**c**) enhanced power system shown to the adversary; (**d**) deliberate attack plan; (**e**) expected power system by the terrorist after attack; (**f**) actual power system after attack.

Figure 3 illustrates the protection strategy in power system fortification, where both agents have equivalent information and the protected branches are invulnerable during attacks. If branches 1–5 and 2–4 are protected, the power system shown in Figure 3c will be derived and seen by both the defender and the attacker. With a budget of attacking two branches, the optimal attack plan shown in Figure 3d will be obtained to isolate node 6, resulting in a broken power system (see Figure 3e). Due to the same perspective of defender and attacker, the actual power system after attack shown in Figure 3f is identical with Figure 3e, where the system power imbalance is positive since node 6 is isolated.

Comparing Figure 2 and Figure 3, the only difference is that branches 1–5 and 2–4 are either hidden or protected. If hidden, the adversary cannot see them; if protected, the adversary cannot destroy them, but they are observable. Therefore, the resulted systems shown to the adversary after deception/protection are different; see Figures 2c and 3c. Although the same attack strategy (e.g., maximizing the system power imbalance) is employed by the attacker, the generated attack plan (Figures 2d and 3d) and the resulting system (Figures 2e and 3e) are different since the target system is distinct. In addition, the actual power system (Figures 2f and 3f) after attack is different. It should be noted that Figure 2 consumes/confronts the same resources/enemies with Figure 3, but the system power imbalance is much lesser, which is mainly due to the deception mechanism, i.e., the power of information asymmetry between the defender and attacker is revealed and harnessed.

2.2. Mathematical Formulation

Following the intrinsic logic of deception in power system fortification revealed above, the target problem can be formulated as a DAD model. In the first stage, the defender proposes an optimal deception scheme with the objective of minimizing the damage will be induced by the attacker. In the second stage, given a deceived power system obtained from the implementation of deception plan, the attacker intends to tear it via tripping power lines with the purpose of maximizing the power imbalance. In the third stage, the defender reacts to the former stages by OPF for the resulted system with the goal of minimizing the unserved energy. Therefore, a tri-level optimization structure for the target problem is given as follows:

$$\min_{x_l} \ \Delta \tag{1}$$

subject to :

$$x_l = \{0,1\}; \forall l \in L \tag{2}$$

$$\sum_{l \in L} x_l \leq N_A \tag{3}$$

$$0 \leq \Delta \leq \bar{\Delta} \tag{4}$$

$$\Delta = \max_{z_l} \Big\{ \delta \tag{5}$$

subject to :

$$z_l = \{0,1\}; \forall l \in L \tag{6}$$

$$\sum_{l \in L} z_l \leq N_B \tag{7}$$

$$z_l \leq 1 - x_l; \forall l \in L \tag{8}$$

$$\delta = \min_{p_i, f_l, S_b^+, S_b^-, \theta_{fr(l)}, \theta_{to(l)}} \Bigg[\sum_{b \in N} \left(S_b^+ + S_b^- \right) \tag{9}$$

subject to :

$$\sum_{i \in I | bu(i) = b} p_i + \sum_{l \in (L) | to(l) = b} f_l - \sum_{l \in (L) | fr(l) = b} f_l - S_b^+ + S_b^- = D_b : (\beta_b); \forall b \in N \tag{10}$$

$$f_l = (1 - x_l - z_l)\gamma_l(\theta_{fr(l)} - \theta_{to(l)}) : (\pi_l); \forall l \in L \tag{11}$$

$$-F_l \leq f_l \leq F_l : (\sigma_l, \phi_l); \forall l \in L \tag{12}$$

$$0 \leq p_i \leq P_i : (\mu_i); \forall i \in I \tag{13}$$

$$S_b^+ \geq 0, S_b^- \geq 0; \forall b \in N \Bigg] \Big\}. \tag{14}$$

The optimization problem (1)–(14) consists of three levels in accordance with DAD model: (1) the upper-level (1)–(5) corresponds to the defender's first stage deception decision; (2) the

middle-level (5)–(9) includes the attacker's second stage attack plan; and (3) the lower-level (9)–(14) is the defender's third stage OPF reaction scheme. Dual variables associated with the lower-level problem are in parentheses. Note that the lower level is parameterized in terms of upper-level variables x_l and middle-level variables z_l.

The objective function (1) to be minimized is the system power imbalance that the attacker can deduce with his/her best effort. Constraints (2) and (3) define the binary nature of deception decision variables and the budget of deception operations. Constraint (4) sets the maximum level of system power imbalance. Equation (5) is both constraint and objective function for the upper-level and middle-level problems, representing the maximum power imbalance after attack. Constraints (6) and (7) model the binary nature of attack variable and its budget bound. Constraint (8) describes that the attack can only be implemented on those branches appeared in the deceived power system, i.e., if $1 - x_l = 0$, the corresponding z_l should be 0 as well. Equation (9) formulates the minimal unserved energy after deception and attack. Constraint (10) represents the nodal power balance equations. Based on the DCPF model, constraint (11) establishes the power flow for branches, where coefficients $(1 - x_l - z_l)$ are guaranteed to be nonnegative due to constraints (8). Constraints (12), (13), and (14) enforce the limits for line flow, generation, and power surplus/deficit, respectively.

In Equation (1)–(14), the tri-level optimization problem is joined by the system power imbalance, which is defined in Equation (9) and calculated via Equation (10). In order to achieve the nodal power balance shown in (10), S_b^+ and S_b^- are included as slack variables. In (10), if the left-hand side is smaller than the right-hand side, then $S_b^+ = 0$ and $S_b^- > 0$; otherwise, $S_b^+ > 0$ and $S_b^- = 0$. Therefore, $\sum_{b \in N} \left(S_b^+ + S_b^-\right)$ is defined as a system power imbalance in this paper, whose interpretation includes power mismatch and load shed as well.

In terms of conventional protection problems, the formulation can be easily revised from (1)–(14) with the following three steps:

1. Change the definition of binary decision variables x_l. Let $x_l = 1$ represent the protection of line l, and vice versa.
2. Delete the constraint (8). Since all the lines are visible for the adversary, each line l is attackable no matter $x_l = 1$ or not.
3. Revise the constraint (11). It is assumed that the protected line cannot be destroyed, i.e., if $x_l = 1$, the power flow of line l is guaranteed to be nonzero whatever the attack z_l is conducted or not. Therefore, constraint (11) can be reformulated as

$$f_l = (1 - z_l + x_l z_l)\gamma_l(\theta_{fr(l)} - \theta_{to(l)}) : (\pi_l); \forall l \in L. \tag{15}$$

Based on the above processes, the optimal protection strategy problem is formulated as

$$\min_{x_l} \ \Delta \tag{16}$$

$$\textit{subject to}:$$

$$\textit{Constraints}\ (2)\text{–}(7),\ (9)\text{–}(10),\ (12)\text{–}(14), (15). \tag{17}$$

It should be noted that the above tri-level optimization problems (1)–(14) and (16)–(17) are just simple mathematical formulations for demonstration, they can be easily extended to include more details, such as the cost in the objective function and more realistic constraints.

3. Solution Methodology

In this section, the developed tri-level MILP problem (1)–(14) will be tackled with two-stage RO algorithm and CCG strategy, resulting in a master-subproblem solution framework, where Δ constitutes the recourse function. The master problem provides a lower bound for the system power

imbalance and generates a deception scheme. Due to feedback mechanism from subproblem, the number of constraints in master problems keeps increasing as the iteration goes on, thus the lower bound is monotonically increasing. On the other hand, the subproblem yields the worst attack plan for a given deceived power system, producing an upper bound for the target problem. The solution process terminates when these two bounds merge into a predefined value ϵ, e.g., 10^{-2}. The convergence of RO and CCG are guaranteed in a finite number of iterations—for more details, please refer to [29] and [21]. In addition, the distance between these two bounds can be utilized to identify the quality of intermediate solutions at each iteration.

3.1. Subproblem

At each iteration k, the subproblems (5)–(14) maximize the system power imbalance Δ for the deceived power system resulting from the upper-level deception plan. Therefore, the subproblem is parameterized by the upper-level decision variables x_l. Nevertheless, the mixed-integer bilinear *max-min* problem is intractable for most off-the-shelf solvers. Fortunately, it can be reformulated into single-level MILP, which is suitable for various solvers, e.g., Cplex, Matlab, and Lingo, etc., based on dual theory or Karush–Kuhn–Tucker (KKT) conditions.

Based on dual theory, the single-level equivalent of the subproblem is obtained as follows:

$$\Delta = \max_{z_l,\beta_b,\pi_l,\sigma_l,\phi_l,\mu_i} \left\{ \sum_{b\in N} D_b\beta_b - \sum_{l\in(L_A\cup L_B)} F_l\sigma_l - \sum_{l\in(L_A\cup L_B)} F_l\phi_l - \sum_{i\in I} P_i\mu_i \right\} \tag{18}$$

$$\textit{subject to}:$$

$$z_l = \{0,1\}; \forall l \in L \tag{19}$$

$$\sum_{l\in L} z_l \le N_B \tag{20}$$

$$z_l \le 1 - x_l^{(j)}; \forall l \in L \tag{21}$$

$$\beta_{bu(i)} - \mu_i \le 0; \forall i \in I \tag{22}$$

$$\beta_{to(l)} - \beta_{fr(l)} + \pi_l + \sigma_l - \phi_l = 0; \forall l \in L \tag{23}$$

$$-1 \le \beta_b \le 1; \forall b \in N \tag{24}$$

$$\sum_{l\in L|to(l)=b} \left(1 - x_l^{(j)} - z_l\right)\gamma_l\pi_l - \sum_{l\in L|fr(l)=b} \left(1 - x_l^{(j)} - z_l\right)\gamma_l\pi_l = 0; \forall b \in N \tag{25}$$

$$\sigma_l, \phi_l \ge 0; \forall l \in L \tag{26}$$

$$\mu_i \ge 0; \forall i \in I, \tag{27}$$

where constraints (19)–(21) are in accordance with middle-level constraints (6)–(8), whereas (22)–(25) are the dual constraints corresponding to primal variables p_i, f_l, $\{S_b^+,\ S_b^-\}$, and θ, respectively.

It is noticeable that constraints (25) are nonlinear due to the products between middle-level binary variables and lower-level dual continuous variables. In order to facilitate the linear solver, linearizion process is implemented on (25), resulting in the following constraints:

$$\sum_{l\in L|to(l)=b} \left[\left(1 - x_l^{(j)}\right)\gamma_l\pi_l - \gamma_l\tau_l\right] - \sum_{l\in L|fr(l)=b} \left[\left(1 - x_l^{(j)}\right)\gamma_l\pi_l - \gamma_l\tau_l\right] = 0; \forall b \in N \tag{28}$$

$$-\bar{\pi}_l(1 - z_l) \le \tau_l - \pi_l \le \bar{\pi}_l(1 - z_l); \forall l \in L \tag{29}$$

$$-\bar{\pi}_l z_l \le \tau_l \le \bar{\pi}_l z_l; \forall l \in L, \tag{30}$$

where $\tau_l = z_l\pi_l$ are new variables to represent the nonlinear terms; constraints (29)–(30) are utilized to achieve the equivalence.

The subproblem of conventional optimal protection strategy problem is similar to (18)–(27) except that the coefficients in constraints (25) should be revised as (31) according to (15). Correspondingly, the linearized constraints (28) should be changed as (32) as well:

$$\sum_{l\in L|to(l)=b}\left(1-z_l+x_l^{(j)}z_l\right)\gamma_l\pi_l-\sum_{l\in L|fr(l)=b}\left(1-z_l+x_l^{(j)}z_l\right)\gamma_l\pi_l=0;\forall b\in N, \tag{31}$$

$$\sum_{l\in L|to(l)=b}\left(\gamma_l\pi_l-\gamma_l\tau_l+x_l^{(j)}\gamma_l\tau_l\right)-\sum_{l\in L|fr(l)=b}\left(\gamma_l\pi_l-\gamma_l\tau_l+x_l^{(j)}\gamma_l\tau_l\right)=0;\forall b\in N. \tag{32}$$

Therefore, the subproblem of optimal protection strategy problem can be summarized as

$$\Delta=\max_{z_l,\beta_b,\pi_l,\sigma_l,\phi_l,\mu_i,\tau_l}\left\{\sum_{b\in N}D_b\beta_b-\sum_{l\in(L_A\cup L_B)}F_l\sigma_l-\sum_{l\in(L_A\cup L_B)}F_l\phi_l-\sum_{i\in I}P_i\mu_i\right\}, \tag{33}$$

$$\begin{aligned}&subject\ to:\\&Constraints\ (19)\text{–}(24),\ (26)\text{ and }(27),(29)\text{ and }(30),\ (32).\end{aligned} \tag{34}$$

3.2. Master Problem

According to the CCG algorithm, the master problem of the optimal deception strategy problem can be generated as follows:

$$\min_{x_l,p_i^m,f_l^m,S_b^{+m},S_b^{-m},\theta_{fr(l)}^m,\theta_{to(l)}^m}\ \Delta \tag{35}$$

$$subject\ to:$$

$$Constraints\ (2)\text{–}(4) \tag{36}$$

$$\Delta\geq\sum_{b\in N}\left(S_b^{+m}+S_b^{-m}\right);m=1,\ldots,j-1 \tag{37}$$

$$\sum_{i\in I_b}p_i^m+\sum_{l\in(L)|to(l)=b}f_l^m-\sum_{l\in(L)|fr(l)=b}f_l^m-S_b^{+m}+S_b^{-m}=D_b;\forall b\in N,m=1,\ldots,j-1 \tag{38}$$

$$f_l^m=(1-x_l-z_l^m)\gamma_l(\theta_{fr(l)}^m-\theta_{to(l)}^m);\forall l\in L,m=1,\ldots,j-1 \tag{39}$$

$$-F_l\leq f_l^m\leq F_l;\forall l\in L,m=1,\ldots,j-1 \tag{40}$$

$$0\leq p_i^m\leq P_i;\forall i\in I,m=1,\ldots,j-1 \tag{41}$$

$$S_b^{+m}\geq 0,S_b^{-m}\geq 0;\forall b\in N,m=1,\ldots,j-1, \tag{42}$$

where m is the number of iterations. It should be noted that the scale of the master problem is increasing at each iteration with constraints (36)–(42) and decision variables p_i^m, f_l^m, S_b^{+m}, S_b^{-m}, $\theta_{fr(l)}^m$, and $\theta_{to(l)}^m$.

It is noticeable that constraint (39) is nonlinear due to the product term $x_l\theta^m$. According to constraint (21), the term $(1-x_l-z_l^m)$ in constraints (39) should be nonnegative. Nevertheless, in the current form of (39), the nonnegative is not guaranteed, e.g., if $x_l=1$ and $z_l^m=1$, there is $1-x_l-z_l^m=-1$, which means that the attack is conducted on a hidden line, but the result is equivalent with building a new line since $f_l^m=-\gamma_l(\theta_{fr(l)}^m-\theta_{to(l)}^m)$. Admittedly, constraint (39) is inappropriate, thus a reformulation is inevitable. In order to achieve the most concise form, the logic relationship between f_l^m, x_l, and z_l^m is summarized in Table 1.

Table 1. Logic relationship between f_l^m, x_l, and z_l^m for the optimal deception strategy problem.

x_l	z_l^m	f_l^m	Explanation
0	0	$\gamma_l(\theta^m_{fr(l)} - \theta^m_{to(l)})$	Line is neither hidden nor attacked.
0	1	0	Line is attacked.
1	0	$\gamma_l(\theta^m_{fr(l)} - \theta^m_{to(l)})$	Line is hidden.
1	1	$\gamma_l(\theta^m_{fr(l)} - \theta^m_{to(l)})$	Line is hidden and attacked.

Based on the Big-M experiences, constraint (39) is linearized as (43) and (44), which are applicable with the logic relationship shown in Table 1. It should be noted that the Big-M in (43) and (44) is valued with $M_l = 2F_l$ due to the nature constraint of f_l:

$$-M_l(1-x_l)z_l^m \le f_l^m - \gamma_l(\theta^m_{fr(l)} - \theta^m_{to(l)}) \le M_l(1-x_l)z_l^m; \forall l \in L_A, m = 1, \ldots, j-1 \quad (43)$$

$$-M_l\left(1-(1-x_l)z_l^m\right) \le f_l^m \le M_l\left(1-(1-x_l)z_l^m\right); \forall l \in L_A, m = 1, \ldots, j-1. \quad (44)$$

Replace constraints (39) with (43) and (44), the MILP master problem is developed. By iteratively solving the master problem and subproblem, their objective function values (corresponding to the lower and upper bounds of the original problem) will merge together, thus the convergence is achieved.

Substitute constraint (39) in (35)–(42) with (45), the master problem of conventional optimal protection strategy problem can be generated. The logic relationship enclosed in (45) between f_l^m, x_l, and z_l^m is identical with Table 1, thus the linearization form of (45) can be represented by (43) and (44) as well. Therefore, the master problem of both optimal deception and protection strategy problems have the same formulation:

$$f_l^m = (1 - z_l^m + x_l z_l^m)\gamma_l(\theta^m_{fr(l)} - \theta^m_{to(l)}); \forall l \in L, m = 1, \ldots, j-1. \quad (45)$$

4. Numerical Experiments

In this section, two cases retrieved from Matpower [30] are employed to validate the proposed model and solution methodology, i.e., the 6-bus system and IEEE 57-bus system. The smaller system is utilized to reveal calculation details and information asymmetry with all power flow data is reported, while the larger system is resorted to perform sensitivity analysis and demonstrate the scalability. Both deception and protection strategies are implemented for comparison and discussion. All simulation tests are coded in Matlab 2018a, called Cplex 12.8.0 with YALMIP [31]. The execution platform is a 64-bit Windows PC with two Intel Core i7-8550U CPU at 1.80 GHz and 16.0 GB of RAM.

4.1. The 6-Bus System

In accordance with the illustrative 6-bus system given in Figures 2 and 3, the configuration and parameter of the original system `case6ww` given in [30] are partially revised. For reproductivity purposes, Tables 2 and 3 present all the input data for the 6-bus system.

Table 2. Generation and load data for the 6-bus system.

Bus No.	Generation P_i (MW)	Load D_b (MW)	Bus No.	Generation P_i (MW)	Load D_b (MW)
1	180	0	4	0	70
2	150	0	5	0	70
3	0	70	6	0	80

Table 3. Branch data for the 6-bus system.

From–To	Reactance (p.u.)	Capacity F_l (MW)	From–To	Reactance (p.u.)	Capacity F_l (MW)
1–2	0.20	80	2–4	0.10	120
1–5	0.30	120	3–4	0.26	80
1–6	0.30	80	4–5	0.40	80
2–3	0.25	80	5–6	0.30	60

Figure 4 depicts the detailed power flow and load shed for both strategies under different defense and attack budgets. If $N_A = N_B = 2$, both strategies intend to hide or protect branches 1–5 and 2–4, nevertheless, the attacked lines are different although the same attack policy is utilized, resulting in the same configurations with Figures 2f and 3f. The reason and stage-wise transformation process have been discussed in Section 2.1, thus Figure 4a,b just reports the results, where full data on the power flow is given for validation. It can be seen that the whole system power imbalance for deception and protection strategies under $N_A = N_B = 2$ is 58.9 MW and 80.0 MW, respectively. In order to further reveal the difference between these two strategies, the defense budget is increased by 1 in Figure 4c,d, i.e., $N_A = 3$ and $N_B = 2$. Results show that the unserved power has reduced to 20 MW and 60 MW respectively. Therefore, it can be concluded that the deception strategy performances better than the protection strategy under various circumstance; in addition, the deception strategy gains much better performance improvement by adding the defense budget.

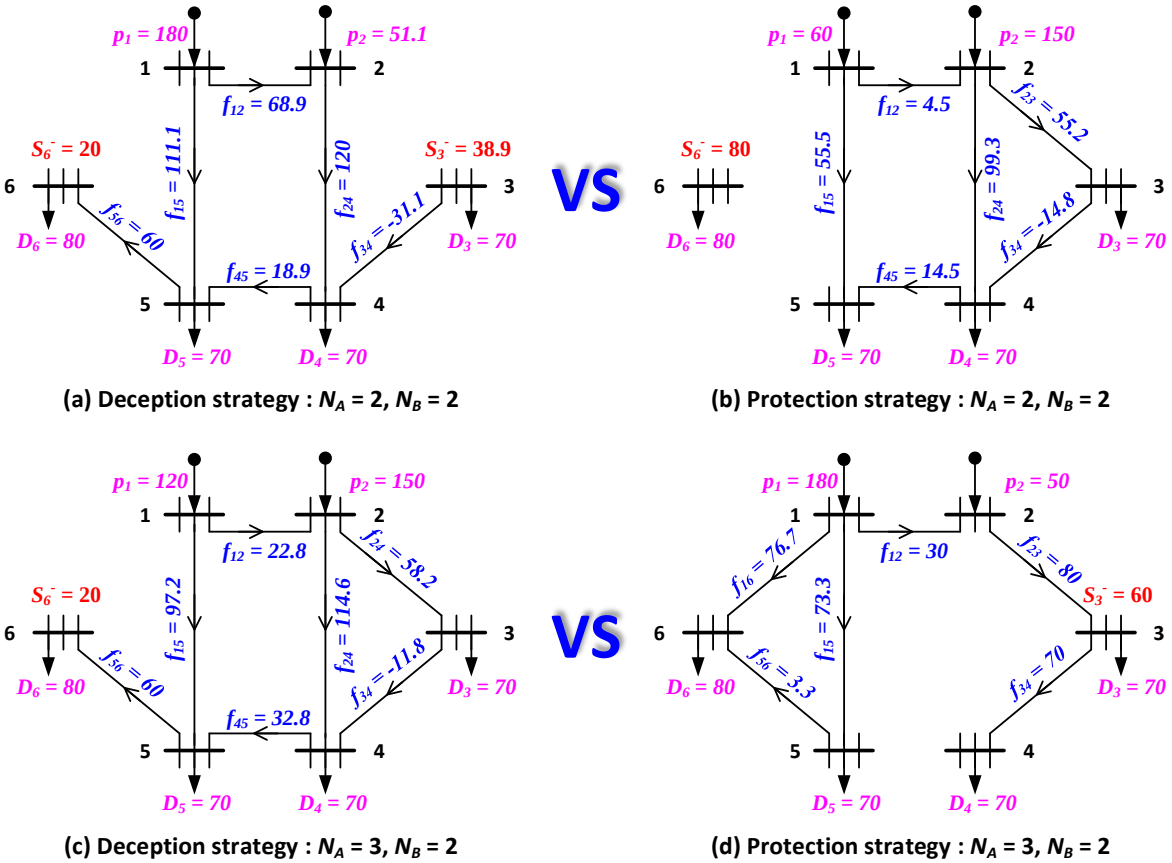
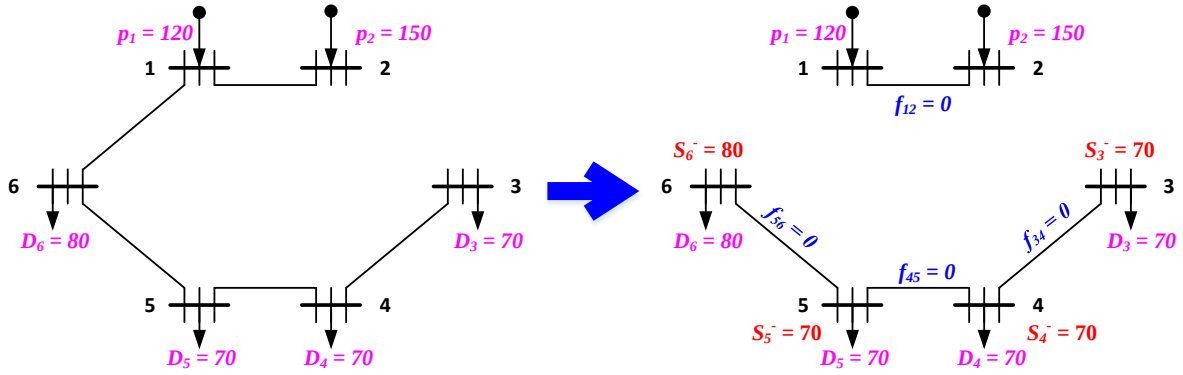


Figure 4. Performance of the optimal deception and protection strategies on the 6-bus system under different defense and attack budgets.

Although results have been reported and discussed in the above, the inner mechanism for Figure 4c,d has not been disclosed. In Figure 4d, the protected branches are 1–5, 1–6, and 2–3. Thus, two lines 2–4 and 4–5 are attacked, resulting in a 60 MW power imbalance at bus 3. The entire

calculation process strictly follows the problem formulation and solution methodology developed for the protection strategy, which are explicitly given in Sections 2 and 3, respectively. In terms of Figure 4c, the hidden branches are 1–5, 2–3, and 2–4, leading to a very fragile system appearing to the enemy. Figure 5a presents the deceived system, where lines 1–6 is the unique branch to connect the generator and load buses. Therefore, the adversary destroyed only one branch (1–6) since breaking other visible lines (1–2, 3–4, 4–5, and 5–6) cannot increase the power imbalance (as all the load buses are isolated, i.e., the maximum unserved power 290 MW is achieved). Figure 5b illustrates the system after attack, where $f_{12} = 0$, $f_{34} = 0$, $f_{45} = 0$, and $f_{56} = 0$, which means that attacking them is not required and does not make any sense. It should be pointed that the comparison between Figure 4c,d is fair since the attack strategy is the same, although the finally implemented attack times are different. In order to achieve "fair" comparison, four more attack plans are enumerated in Table 4. It can be observed that the system power imbalance is less than 60 MW (the protection strategy) for the majority of attack plans, and the average is only 34 MW, thus the deception strategy still gains superiority.



(a) Deceived system shown to the adversary **(b) Resulted system after attack**

Figure 5. Intermediate systems for the deception strategy with $N_A = 3$ and $N_B = 2$.

Table 4. System power imbalance under different attack plans.

Attack Plans	Node Power Imbalance (MW)	System Power Imbalance (MW)
1–6	$S_6^- = 20$	20
1–6 & 1–2	$S_6^- = 20$	20
1–6 & 3–4	$S_6^- = 20$	20
1–6 & 4–5	$S_5^- = 10, S_6^- = 20$	30
1–6 & 5–6	$S_6^- = 80$	80
	Average	34

4.2. IEEE 57-Bus System

The dataset of IEEE 57-bus system is fetched from [30]; however, the power flow capacity of each branch is incomplete, thus we randomly generated F_l for each line with the following equation:

$$F_l = 70 + round(10r_l), \tag{46}$$

where $r_l \in [0, 1]$ is a random number subject to uniform distribution, $round()$ is the rounding function. It should be noted that $F_l \in [70, 80]$ pushes the system into a critical point, i.e., the power balance is achievable under normal state, but power imbalance is easy to appear if some branches are attacked. For the purpose of quick reference, all data related to IEEE 57-bus system are attached in Appendix A, and the single line diagram is given in Figure 6.

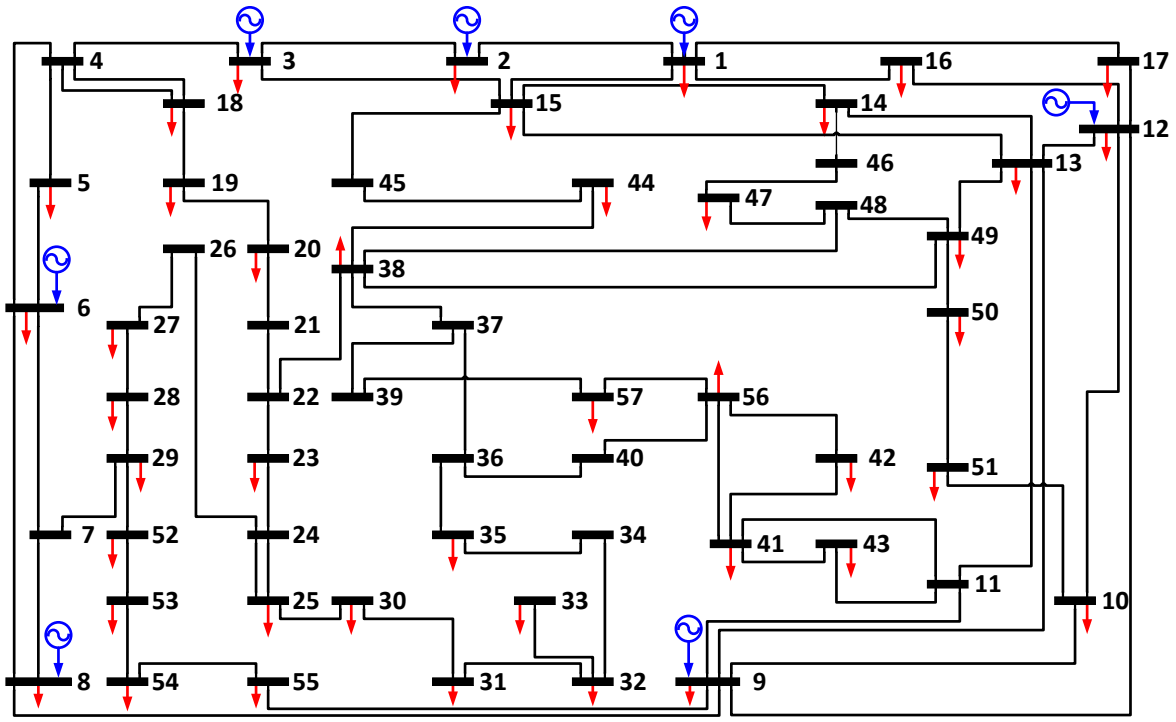


Figure 6. Single line diagram of the IEEE 57-bus system.

4.2.1. Performance Evaluation

In order to further identify the difference between two strategies, a lot of experiments are implemented on the IEEE 57-bus system under different defense and attack budgets, i.e., corresponding to various numbers of N_A and N_B. All results are summarized in Table 5. To facilitate the description, Figure 7 illustrates the results of protection strategy. At point D ($N_A = N_B = 0$), the power imbalance Δ is 0, indicating that the system is sufficient in the original status. From point D to A, the maximum number of attacks is increasing while the protection budget is fixed, thus Figure 7 demonstrates a monotonically increasing trend on the unserved power. On the other hand, from point A to B, the defense budget is increasing, but the attack strength is constant, resulting in a monotonically reducing trend on the system power imbalance, which is observable in Figure 7. Therefore, it can be concluded that the elimination of power imbalance from A to B and D is due to the increase of defense budget N_A and the decrease of attack capability N_B, respectively. However, the decrease rate is different since $\Delta(B)$ is 151.9 MW while $\Delta(D)$ is 0 MW, showing that the variation of N_B has a stronger influence on the system power imbalance. This phenomenon can also be partially identified with point B, where a large amount of unserved power has appeared although N_A is equal to N_B. Even if $N_A = 7$ and $N_B = 1$, the system power imbalance shown in Figure 7 is still positive.

Table 5. Power imbalance with both strategies under different defense and attack budgets.

Power Imbalance (MW)		$N_A = 0$	$N_A = 1$	$N_A = 2$	$N_A = 3$	$N_A = 4$	$N_A = 5$	$N_A = 6$	$N_A = 7$
Protection Strategy	$N_B = 0$	**0.00, D**	0.00	0.00	0.00	0.00	0.00	0.00	**0.00, C**
	$N_B = 1$	66.96	48.42	46.13	41.93	41.61	31.04	17.67	14.23
	$N_B = 2$	115.29	104.52	99.75	90.70	79.51	51.73	46.02	39.00
	$N_B = 3$	171.23	162.78	148.01	131.82	108.05	77.23	65.73	55.47
	$N_B = 4$	226.82	219.86	200.78	158.60	123.24	114.65	81.91	81.11
	$N_B = 5$	295.74	274.45	228.60	187.60	167.58	138.34	114.43	100.10
	$N_B = 6$	305.60	297.60	257.60	221.68	180.13	162.60	143.93	131.02
	$N_B = 7$	**376.6, A**	327.80	279.60	236.60	212.44	188.80	168.47	**151.9, B**
Deception Strategy	$N_B = 0$	**0.00, D**	0.00	0.00	0.00	0.00	0.00	0.00	**0.00, C**
	$N_B = 1$	66.96	46.13	41.61	41.61	31.04	3.68	3.68	0.00
	$N_B = 2$	115.29	104.52	90.83	79.51	35.63	35.63	24.96	3.68
	$N_B = 3$	171.23	159.35	147.20	95.35	85.53	58.00	34.16	14.02
	$N_B = 4$	226.82	219.86	153.60	145.60	109.76	70.31	35.84	40.29
	$N_B = 5$	295.74	226.60	221.60	172.80	124.15	70.31	38.34	41.23
	$N_B = 6$	305.60	297.60	248.80	185.80	124.15	70.86	48.38	44.34
	$N_B = 7$	**376.6, A**	324.80	261.80	185.80	125.20	79.72	69.61	**46.72, B**

A, **B**, **C**, **D**: Points will be utilized in Figures 7–9 to facilitate the description.

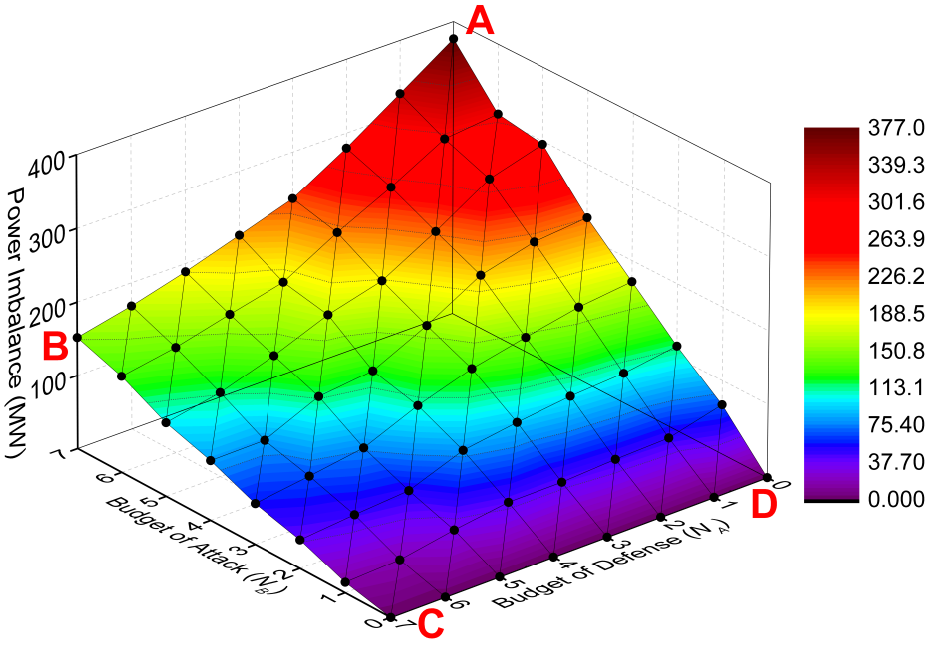


Figure 7. Power imbalance with the protection strategy under different defense and attack budgets.

Figure 8 presents the results with deception strategy, where similar trends with Figure 7 from point A to B and D are observable. The power imbalance levels from point A to D (where $N_A = 0$, i.e., there is no protection or deception) reported in Figure 8 are identical to Figure 7, indicating that the attack policy is the same. Nevertheless, the point B shown in Figure 8 is much lower than Figure 7, which means that the deception gains have better performance than the protection strategy. Actually, all points shown in Figure 8 are less than or equal to Figure 7. As discussed in Figure 7, Δ is positive at point $(N_A, N_B) = (7, 1)$; nevertheless, $\Delta = 0$ is achieved in Figure 8.

Based on the above comparison, the superiority of deception strategy over protection strategy is established. In order to further investigate the differences between these two strategies, Figure 9 is generated, where the data at each point are obtained from the substitution of corresponding points shown in Figures 7 and 8. Firstly, all points are nonnegative, which is expected according to the above analysis. Then, an interesting observation is that the variation is higher as N_A and N_B are larger. Bigger

values of N_A and N_B mean larger solution space and more system flexibility, indicating that the full potential of deception strategy is easier to be fulfilled with complicated problems.

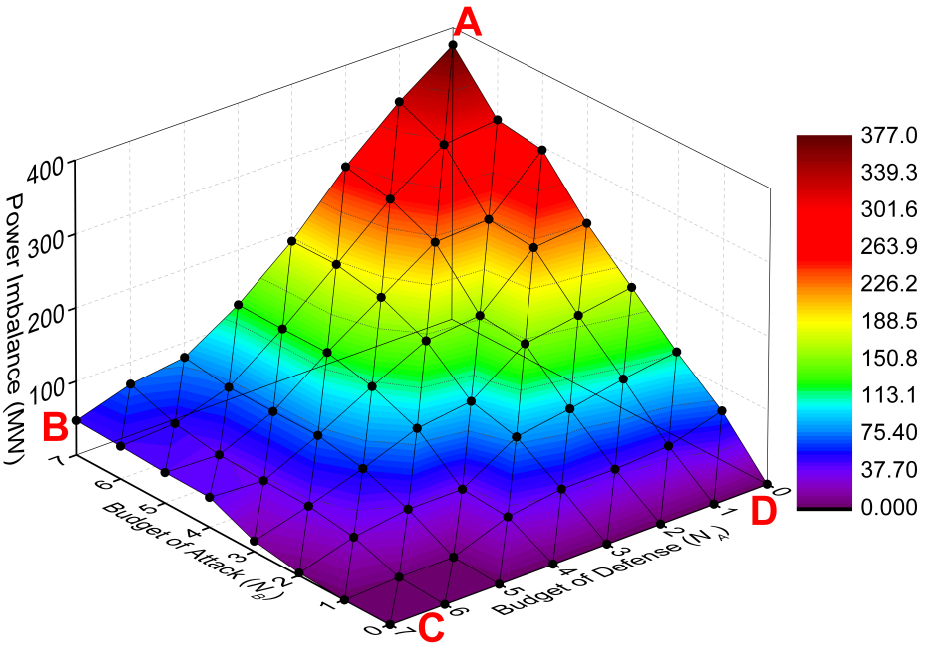


Figure 8. Power imbalance with the deception strategy under different defense and attack budgets.

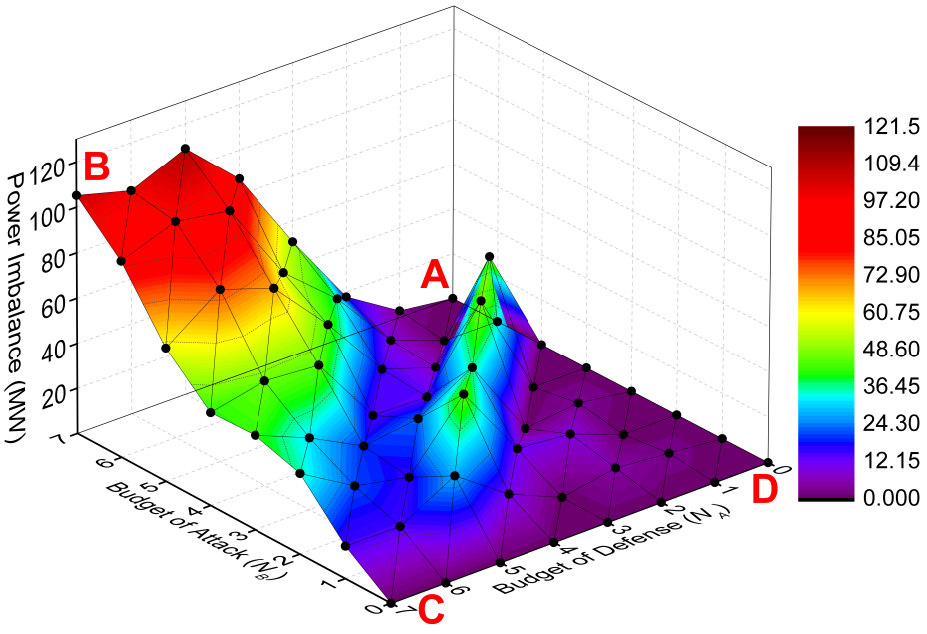


Figure 9. Difference of power imbalance with various fortification strategies under different defense and attack budgets.

4.2.2. Convergence Analysis

In this subsection, the convergence property of both strategies is analyzed in three specified scenarios. Since both N_A and N_B are valued in $[0,7]$, there are 64 combinations to generate experiment scenario. In this case study, three complicated (large N_A and N_B) but balanced (N_A is equal to N_B) are determined as testbed, i.e., Scenario A ($N_A = N_B = 5$), Scenario B ($N_A = N_B = 6$), and Scenario C

($N_A = N_B = 7$). Figure 10 illustrates the convergence property of deception and protection strategies under different scenarios. The difference on power imbalance level is obvious, and the reason has been discussed in the above subsection. Both strategies achieved the convergence under a finite number of iterations, but the convergence rate is different. Deception strategy finished the calculation within 10 iterations, while 30–60 iterations are required to eliminate the gap between lower and upper bounds. If the scale of master problems and subproblems are fixed, then the execution time will linearly increase as iteration goes on. Nevertheless, the scale of master problem is increasing since CCG constraints will be iteratively included, i.e., more time is required to solve the master problem in latter iterations; therefore, the whole execution time increase rate would be super-linear, which is validated with the comparison between deception and protection strategies. The reason for the smaller number of iterations with deception strategy might be explained from two aspects: (1) the hidden lines reduced the solution space of the subproblem, resulting in the worst attack plan being easy to be found; (2) the hidden lines changed the configuration of subproblem solution space, leading to the CCG constraints being capable of eliminating more intermediate solutions; and (3) the variation on objectives between defender and attacker makes their decisions be diametrically opposed, resulting in the room for bargaining is limited, thus the number of iterations is smaller.

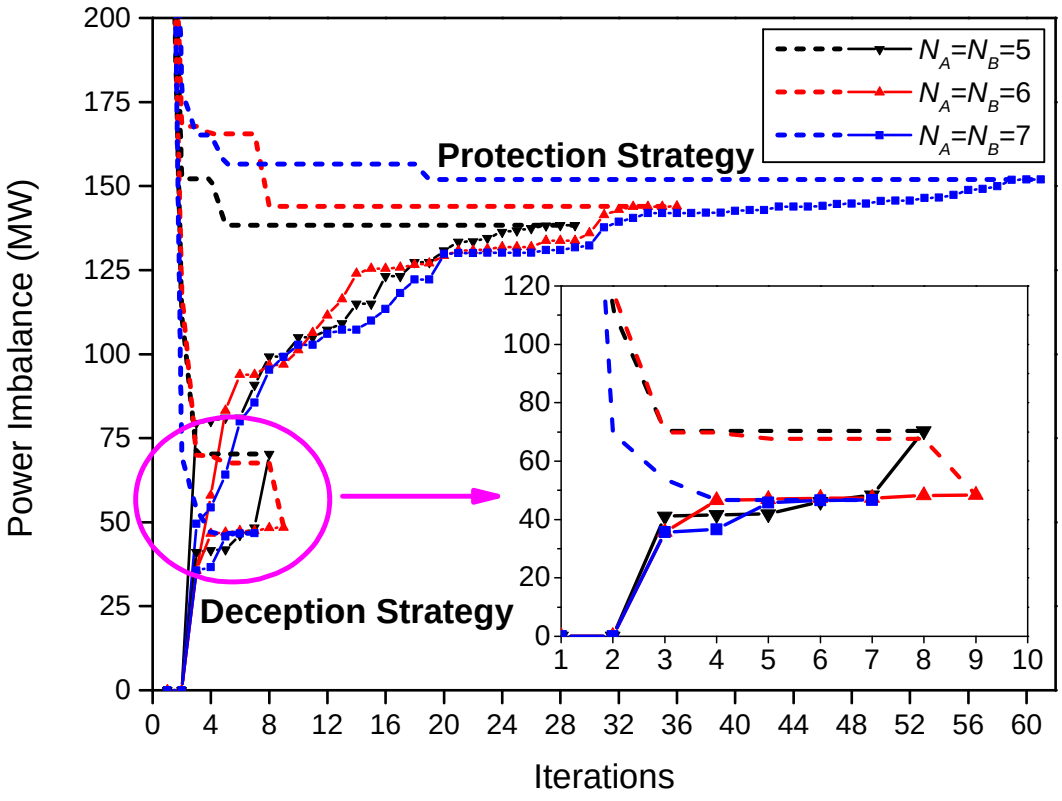


Figure 10. Convergence property of deception and protection strategies.

5. Conclusions

The power system fortification problem against deliberate attacks is investigated in this paper. Different from traditional protection strategy, where the attacker is assumed to be capable of accessing sufficient information, including network topology, device parameters, physical capacity, and defensive decision, the information asymmetry between defender and attacker is introduced in this work, resulting in an optimal deception strategy problem. In order to explicitly reveal the advantageous and significance of information in the two-player game, both deception and protection strategies are described in detail with the invented 6-bus system, formulated into the tri-level MILP problem, and solved via two-stage RO and CCG algorithms. Numerical experiments are carried out on both the 6-bus

system and the IEEE 57-bus system. In the first network, numerical validation of the superiority of deception is presented. On the other hand, performance evaluation and convergence analysis are given based on the second grid. Although deception strategy is integrated into power system fortification, the considered defensive operation is still limited. In the future, more comprehensive deception and attack strategies will be investigated, e.g., setting up fake components (including transmission lines, generators, and loads, etc.), concealing critical loads, and attacking nodes in addition to branches, etc. In addition, different from binary metrics, the success rate/probability of deception and protection operation implemented on each branch will be included in the solution framework.

Author Contributions: Investigation, P.J.; Methodology, P.J.; Supervision, T.Z.; Validation, S.H.; Writing—Original Draft, S.H.; Writing—Review and Editing, T.Z.

Funding: This work was supported by the Distinguished Natural Science Foundation of Hunan Province (No. 2017JJ1001) and the National Natural Science Foundation of China (Nos. 61773390, 71571187). This work was also supported by the China Postdoctoral Science Foundation (No. 2017M623381).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AD	Attacker–Defender
AMI	Advanced Metering Infrastructure
CCG	Column-and-Constraint Generation
DAD	Defender-Attacker-Defender
FDIA	False Data Injection Attack
IED	Intelligent Electronic Device
KKT	Karush–Kuhn–Tucker
LP	Linear Programming
MILP	Mixed-Integer Linear Programming
RO	Robust Optimization
SCADA	Supervisory Control And Data Acquisition

Nomenclature

Δ	System power imbalance, given x_l.
$\mathrm{e}x_l$	Binary variable that is equal to 1 if line l is hidden for deception; being 0 otherwise.
L	Set of branch indexes.
N_A	Maximum number of lines can be hidden for deception.
$\bar{\Delta}$	Maximum level of system power imbalance.
δ	System power imbalance, given x_l, and z_l.
z_l	Binary variable that is equal to 1 if line l is attacked; being 0 otherwise.
N_B	Maximum number of lines can be attacked.
p_i	Power output of generator i.
$bu(i)$	The bus that generator i is connected to.
f_l	Power flow of line l.
$fr(l)$	Sending or origin bus of line l.
$to(l)$	Receiving or destination bus of line l.
S_b^+	Power surplus at bus b.
S_b^-	Power deficit at bus b.
D_b	Demand at bus b.
N	Set of bus indexes.
γ_l	Suspectance of line l.
θ_b	Phase angle at bus b.
F_l	Power flow capacity of line l.
P_i	Capacity of generator i.
I	Set of generator indexes.

Appendix A. The Dataset of IEEE 57-Bus System

For the purpose of quick reference and reproductivity, the generation, load, and branch data of IEEE 57-bus system are reported in Tables A1 and A2.

Table A1. Generation and load data for IEEE 57-bus system.

Bus No.	P_i (MW)	D_b (MW)	Bus No.	P_i (MW)	D_b (MW)	Bus No.	P_i (MW)	D_b (MW)
1	575.88	55	20	0	2.3	39	0	0
2	100	3	21	0	0	40	0	0
3	140	41	22	0	0	41	0	6.3
4	0	0	23	0	6.3	42	0	7.1
5	0	13	24	0	0	43	0	2
6	100	75	25	0	6.3	44	0	12
7	0	0	26	0	0	45	0	0
8	550	150	27	0	9.3	46	0	0
9	100	121	28	0	4.6	47	0	29.7
10	0	5	29	0	17	48	0	0
11	0	0	30	0	3.6	49	0	18
12	410	377	31	0	5.8	50	0	21
13	0	18	32	0	1.6	51	0	18
14	0	10.5	33	0	3.8	52	0	4.9
15	0	22	34	0	0	53	0	20
16	0	43	35	0	6	54	0	4.1
17	0	42	36	0	0	55	0	6.8
18	0	27.2	37	0	0	56	0	7.6
19	0	3.3	38	0	14	57	0	6.7

Table A2. Branch data for IEEE 57-bus system.

From–To	Re. (p.u.)	F_l (MW)	From–To	Re. (p.u.)	F_l (MW)	From–To	Re. (p.u.)	F_l (MW)
1–2	0.0280	72	14–15	0.0547	76	41–42	0.3520	79
2–3	0.0850	71	18–19	0.6850	73	41–43	0.4120	75
3–4	0.0366	79	19–20	0.4340	78	38–44	0.0585	70
4–5	0.1320	71	21–20	0.7767	73	15–45	0.1042	77
4–6	0.1480	74	21–22	0.1170	80	14–46	0.0735	74
6–7	0.1020	79	22–23	0.0152	77	46–47	0.0680	78
6–8	0.1730	77	23–24	0.2560	80	47–48	0.0233	72
8–9	0.0505	75	24–25	1.1820	79	48–49	0.1290	77
9–10	0.1679	70	24–25	1.2300	72	49–50	0.1280	75
9–11	0.0848	70	24–26	0.0473	73	50–51	0.2200	73
9–12	0.2950	78	26–27	0.2540	77	10–51	0.0712	71
9–13	0.1580	70	27–28	0.0954	70	13–49	0.1910	70
13–14	0.0434	70	28–29	0.0587	80	29–52	0.1870	75
13–15	0.0869	75	7–29	0.0648	76	52–53	0.0984	79
1–15	0.0910	72	25–30	0.2020	76	53–54	0.2320	79
1–16	0.2060	79	30–31	0.4970	72	54–55	0.2265	77
1–17	0.1080	76	31–32	0.7550	72	11–43	0.1530	72
3–15	0.0530	71	32–33	0.0360	78	44–45	0.1242	77
4–18	0.5550	72	34–32	0.9530	75	40–56	1.1950	72
4–18	0.4300	70	34–35	0.0780	76	56–41	0.5490	78
5–6	0.0641	73	35–36	0.0537	74	56–42	0.3540	71
7–8	0.0712	80	36–37	0.0366	73	39–57	1.3550	77
10–12	0.1262	72	37–38	0.1009	72	57–56	0.2600	78
11–13	0.0732	71	37–39	0.0379	77	38–49	0.1770	77
12–13	0.0580	73	36–40	0.0466	73	38–48	0.0482	74
12–16	0.0813	72	22–38	0.0295	73	9–55	0.1205	75
12–17	0.1790	73	11–41	0.7490	78			

References

1. Boyer, S.A. *SCADA: Supervisory Control and Data Acquisition*; International Society of Automation: Pittsburgh, PA, USA, 2009.
2. Chen, C.; Wang, J.; Qiu, F.; Zhao, D. Resilient distribution system by microgrids formation after natural disasters. *IEEE Trans. Smart Grid* **2016**, *7*, 958–966. [CrossRef]
3. Yuan, W.; Wang, J.; Qiu, F.; Chen, C.; Kang, C.; Zeng, B. Robust optimization-based resilient distribution network planning against natural disasters. *IEEE Trans. Smart Grid* **2016**, *7*, 2817–2826. [CrossRef]
4. Xu, X.; Mitra, J.; Cai, N.; Mou, L. Planning of reliable microgrids in the presence of random and catastrophic events. *Int. Trans. Electr. Energy Syst.* **2014**, *24*, 1151–1167. [CrossRef]
5. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr. Power Syst. Res.* **2017**, *149*, 156–168. [CrossRef]
6. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
7. Bilis, E.I.; Kröger, W.; Nan, C. Performance of electric power systems under physical malicious attacks. *IEEE Syst. J.* **2013**, *7*, 854–865. [CrossRef]
8. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-Physical System Security for the Electric Power Grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]
9. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
10. Zhu, Y.; Yan, J.; Tang, Y.; Sun, Y.L.; He, H. Joint substation-transmission line vulnerability assessment against the smart grid. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1010–1024. [CrossRef]
11. Wang, Z.; He, J.; Nechifor, A.; Zhang, D.; Crossley, P. Identification of critical transmission lines in complex power networks. *Energies* **2017**, *10*, 1294. [CrossRef]
12. Zhang, G.; Li, Z.; Zhang, B.; Qiu, D.; Halang, W.A. Cascading failures of power grids caused by line breakdown. *Int. J. Circuit Theory Appl.* **2015**, *43*, 1807–1814. [CrossRef]
13. Wenli, F.; Zhigang, L.; Ping, H.; Shengwei, M. Cascading failure model in power grids using the complex network theory. *IET Gener. Transm. Distrib.* **2016**, *10*, 3940–3949. [CrossRef]
14. Zhao, L.; Zeng, B. Vulnerability analysis of power grids with line switching. *IEEE Trans. Power Syst.* **2013**, *28*, 2727–2736. [CrossRef]
15. Li, Z.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. Bilevel model for analyzing coordinated cyber-physical attacks on power systems. *IEEE Trans. Smart Grid* **2016**, *7*, 2260–2272. [CrossRef]
16. Tan, Y.; Li, Y.; Cao, Y.; Shahidehpour, M. Cyber-Attack on Overloading Multiple Lines: A Bilevel Mixed-Integer Linear Programming Model. *IEEE Trans. Smart Grid* **2018**, *9*, 1534–1536. [CrossRef]
17. Lai, K.; Illindala, M.; Subramaniam, K. A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. *Appl. Energy* **2019**, *235*, 204–218. [CrossRef]
18. Yao, Y.; Edmunds, T.; Papageorgiou, D.; Alvarez, R. Trilevel optimization in power network defense. *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.* **2007**, *37*, 712–718. [CrossRef]
19. Ding, T.; Yao, L.; Li, F. A multi-uncertainty-set based two-stage robust optimization to defender–attacker–defender model for power system protection. *Reliab. Eng. Syst. Saf.* **2018**, *169*, 179–186. [CrossRef]
20. Zhao, L.; Zeng, B. Robust unit commitment problem with demand response and wind energy. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; pp. 1–8.
21. Zeng, B.; Zhao, L. Solving two-stage robust optimization problems using a column-and-constraint generation method. *Oper. Res. Lett.* **2013**, *41*, 457–461. [CrossRef]
22. Ruiz, C.; Conejo, A.J. Robust transmission expansion planning. *Eur. J. Oper. Res.* **2015**, *242*, 390–401. [CrossRef]
23. Lorca, A.; Sun, X.A. Adaptive robust optimization with dynamic uncertainty sets for multi-period economic dispatch under significant wind. *IEEE Trans. Power Syst.* **2015**, *30*, 1702–1713. [CrossRef]
24. Huang, S.; Dinavahi, V. A comparison of implicit and explicit methods for contingency constrained unit commitment. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 September 2017; pp. 1–6.

25. Lee, C.; Liu, C.; Mehrotra, S.; Bie, Z. Robust Distribution Network Reconfiguration. *IEEE Trans. Smart Grid* **2015**, *6*, 836–842. [CrossRef]
26. Costa, A.; Georgiadis, D.; Ng, T.S.; Sim, M. An optimization model for power grid fortification to maximize attack immunity. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 594–602. [CrossRef]
27. Ouyang, M.; Xu, M.; Zhang, C.; Huang, S. Mitigating electric power system vulnerability to worst-case spatially localized attacks. *Reliab. Eng. Syst. Saf.* **2017**, *165*, 144–154. [CrossRef]
28. Wu, X.; Conejo, A.J. An efficient tri-level optimization model for electric grid defense planning. *IEEE Trans. Power Syst.* **2017**, *32*, 2984–2994. [CrossRef]
29. Bertsimas, D.; Brown, D.B.; Caramanis, C. Theory and applications of robust optimization. *SIAM Rev.* **2011**, *53*, 464–501. [CrossRef]
30. Zimmerman, R.D.; Murillo-Sanchez, C.E.; Thomas, R.J. MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Trans. Power Syst.* **2011**, *26*, 12–19. [CrossRef]
31. Löfberg, J. YALMIP: A Toolbox for Modeling and Optimization in MATLAB. In Proceedings of the 2004 IEEE International Conference on Robotics and Automation, New Orleans, LA, USA, 2–4 September 2004; pp. 284–289.

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).