Defense Strategy Against Load Redistribution Attacks on Power Systems Considering Insider Threats

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

***Abstract*—In recent years, cybersecurity is emerging as one of the most critical problems to the normal operation of power systems. Meanwhile, insider threats are considered as a strategic and serious challenge in the cybersecurity research and have attracted increasing attention. In this article, the detailed model of load redistribution (LR) attacks against the power systems considering the presence of insider threats is developed. The LR attack problem is formulated with a security resource allocation game model. Information leakage of the system operator's defense strategy by the insider to the external attacker is considered in the proposed game model. The optimal strategies of both the system operator and attacker in the presence of the insider are calculated to maximize their own payoffs. In so doing, the impacts of the insider in the LR attacks can be investigated with the proposed security resource allocation game model. Case studies based on the IEEE 39-bus and IEEE 118-bus test systems were conducted to validate the proposed model. The results of the case studies show that the information leakage by the insider will increase the payoff of the attacker in the LR attacks. The damage on the grid can be considerable even if the information leakage probability is small. The proposed defense strategy is able to reduce the expected operation cost of the system under the LR attacks with the information leakage due to the insider threats.**

***Index Terms*—Coordinated attack, false data injection, cyber resilience, information leakage, insider threat, load redistribution attack, power system cybersecurity.**

I. Introduction

IN THE past few decades, cyber systems have been widely implemented in the power systems to improve the efficiency of the system operation [1], [2]. The efficiency of the power system operation is enhanced as collecting, transferring and processing a tremendous amount of data in a short time to monitor, analyze and control the grid become available by the implementation of the cyber systems. The automation of the power system operation is enhanced, necessary labor force is reduced, more tasks can be accomplished, and the power system can be operated at a lower cost with the integrated cyber systems. While the power system is operated more efficiently due to the rapid integration of operation technology (OT) and ICT, cyber vulnerability is introduced across all levels of power systems from the control systems to the local devices by the digital communicating equipment and standard communication protocols [3]. As a result, cybersecurity threats to the power systems are emerging as an urgent issue, and successful cyberattacks on power systems have already been reported in the real world. For instance, in 2015-2016, the Ukraine power grid was struck by cyberattacks twice in less than one year [4]. During the first attack in December 2015, about 225 thousand residents in three provinces of Ukraine were affected and over 130 MW of load were lost [5]. As the potential consequences of successful cyberattacks against the grids can be catastrophic, it is vital to study the mechanism of the cyberattacks on the power systems and investigate effective countermeasures for mitigating such malicious attacks.

In recent years, increasing attention has been paid to the insider threats by both the academia and industry due to the great impacts of insiders to cybersecurity. Surveys and statistics show that a considerable proportion of organizations have experienced insider threats and attacks, which are among the most costly cyberattacks and take longer time to be resolved [6]. In cybersecurity, the insider threats can be from both the malicious insiders and inadvertent insiders. The malicious insiders can be motivated to be complicit in the attacks with the attackers for personal, financial reasons, or revenge. For example, the tipping points of insider events can be employee dismissal, disputes with employers, perceived injustices, negative company acts, family problems, coercion, offers or financial incentives from adversaries [7]. The inadvertent insider threats may exist and be exploited by the attackers due to a lack of training or loose policy in cybersecurity while the inadvertent insiders have no malicious intent [7]–[9]. Therefore, critical information in cybersecurity can be exposed by the insiders to the attackers and cause more damaging consequences in the cyberattacks. In particular, insider threats are fatal to the cybersecurity of power systems. Generally, it is presumed that power systems are less vulnerable to cyberattacks because of the inaccessibility of system knowledge to external attackers and isolation of the control systems to external networks [10]. However, such inherent barriers of power systems against cyberattacks

Manuscript received March 3, 2020; revised July 4, 2020; accepted August 22, 2020. Date of publication September 11, 2020; date of current version February 26, 2021. This work was supported in part by the U.S. National Science Foundation under Award ECCS1711617, and in part by the Research Growth Initiative Program of University of Wisconsin-Milwaukee under Award 101X360. Paper no. TSG-00310-2020. *(Corresponding author: Lingfeng Wang.)*

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

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

Digital Object Identifier 10.1109/TSG.2020.3023426

can easily be overcome by insiders. Insiders such as malicious employees in the electric sector have intimate knowledge of the functions, processes, systems, equipment, and personnel comprising the bulk power system [3]. The presence of insider threats will not only reduce the cost and difficulty for the attempts of performing the attacks but also increase the potential damages of successful cyberattacks against the power systems. Nevertheless, compared with external threats, there is less awareness of the insider threats in power systems and few studies consider insider threats in the cybersecurity of power systems at present. Thus, it is critical to prepare the electric grid for the new phase of cybersecurity against not only the external attacks but also more sophisticated, covert and damaging internal-external coordinated attacks by furnishing critical knowledge of insider threats in power systems.

The false data injection (FDI) attacks are malicious cyberattacks which can seriously jeopardize the state estimation and normal operation of the modern power systems and other cyber-physical systems (CPS) [11]. Thus, recent efforts have been devoted to analyzing the FDI attacks with different focuses. In this article, we focus on the load redistribution (LR) attack on power systems. The LR attack is an important type of FDI attacks against the operation of the grid which draws wide attention in recent years. It was firstly introduced and studied in [12]. In the LR attack, the attacker manipulates the measurements of the load bus injection and line power flow in the grid to mislead the dispatch decisions of the system operator. In doing so, the attacker leads the power system into a false secure and optimal operating state. In [13], a restart framework using Benders decomposition is employed to solve the LR attack problem efficiently. The authors of [14] propose a local LR attack model based on incomplete network information and show that an attacker only needs to obtain the network information of the local attacking region to inject false data into the smart meters in the local region without being detected by the state estimator. The modeling of the LR attack with incomplete network information is also investigated in [15]. In [16], [17], not only the LR attack under incomplete network information is studied, the coordinated cyber-physical attacks on the power grids are also analyzed in the research. In [18], the coordinated local LR attack and topology attack are modeled. A minimax-regret decision rule based model is proposed in [19] to achieve the cost-effective defense strategy for protecting the power systems from the FDI attacks including the LR attack. A bi-level optimization model is proposed in [20] to determine the optimal cybersecurity reinforcement strategies against the LR attack. In [21], a network constrained unit commitment model under the LR attack is proposed with a tri-level optimization model. Meanwhile, a vulnerability analysis framework of the smart grid under the LR attack is proposed in [22]. Further, a framework is proposed to study the coordination between the LR attack and switching attack in [23]. The influence of the LR attack is also considered in the power supply adequacy assessment and power system reliability analysis in literature. The study in [24] incorporates the local LR attack into the conventional power system adequacy assessment. A holistic framework incorporating the physical failures and the LR attack is proposed for the cyber-physical power system reliability evaluation in [25]. As a kind of FDI attacks, the LR attack is performed by injecting false data in the load and power flow measurements in the grid. Compared with other cyberattacks, e.g., switching attacks against the grid [26], which send false commands against the operation of the control system in the grid directly, the attacker of the LR attack does not need to break through more secured and isolated communication layers of the control systems or bypass the protection and interlock commands. Thus, the attacker may face less obstacles and barriers when launching the LR attack on the grid. Therefore, the LR attack is a realistic risk and an important cyberattack model on the power grid that needs to be studied. In this article, a security resource allocation game model is developed for the LR attack. In the proposed model, although the time for the determination of the attack and defense strategies may vary, the influence of the attack and defense actions on the system is simultaneous. Further, the actions of the attacker and defender only influence the outcome of the attack and the system generation dispatch in the current attack. Thus, the static game model is applied in this study instead of a sequential game. Meanwhile, the information leakage by the insider is formulated in the proposed game model to consider the insider threats in the LR attack.

Information leakage is a significant concern in the practical application of security games that can be introduced by the insider threats [27]. The information of the system defense strategy may be exposed to the attacker by the insider so that the payoffs of the attacker can be improved, and consequently the damage of the attack will increase. In the proposed security resource allocation game model of this article, the information leakage of the system operator's strategy by the insider is considered and formulated. The defense and attack strategies of the system operator and attacker in the LR attack with the information leakage by the insider are searched. Accordingly, the expected system operation cost in the LR attack and the impacts of the information leakage by the insiders are studied. Further, the case when there is no information leakage in the game is also considered and compared in the paper. In this case, neither the defender nor the attacker knows the instantiation of the mixed strategy of its opponent. The optimal strategies of the attacker and defender at the Nash equilibrium are obtained. The results of the case studies show that the damage of the LR attack in this case is relatively lower than the cases when the information leakage due to insider threats exists. Thus, the existence of information leakage by insiders is damaging to the power grids under LR attacks. To the best of our knowledge, this is the first study which accounts for the information leakage of the defense strategy by insider threats in the cybersecurity analysis of power grids. The work of this article will provide useful insights to help understand the impacts of information leakage due to the insider threats in the cyberattacks against the normal operation of power systems. The contributions of this article are summarized as follows:

- Development of the security resource allocation game model of the LR attacks on power systems.
- Formulating the information leakage due to the presence of insiders in the security resource allocation game model of the LR attacks on power systems.

- Development of the optimization models to calculate the mixed strategies and payoffs of the system operator and attacker at the Nash Equilibrium of the security resource allocation game model with the information leakage of the defense strategy. The potential damage of the LR attacks on the power systems with the information leakage due to the insider threats can be obtained accordingly.
- Analysis on the impacts of the information leakage by the insider to the payoffs of the system operator and attacker in the LR attacks. The factors of the insider threats which will influence the potential damage of the LR attacks to the grid are studied.

The rest of the paper is organized as follows. The security resource allocation game model of LR attacks on power systems is introduced in Section II. The modeling of the information leakage by insiders in the LR attacks is formulated and presented in Section III. The optimization models to calculate the mixed strategies of the system operator and attacker are presented in the same Section. In Section IV, the case studies are presented and discussed, followed by the conclusions in Section V.

II. Security Resource Allocation Game Model of Load Redistribution Attacks

A. Load Redistribution Attacks on Power Systems

In the LR attack, the attacker injects false data to the load measurements $\boldsymbol{P_L}$ and power flow measurements $\boldsymbol{P_F}$ of the grid to mislead the system operator's decision making on power dispatch. The false data injections into the load and power flow measurements are denoted by $\Delta\boldsymbol{P_L}$ and $\Delta\boldsymbol{P_F}$, respectively. With the contaminated measurements, the system operator performs the power dispatch to minimize the system operation cost. Thus, the LR attack on the power system can be modeled as a bi-level optimization problem. In the upper level problem, the attacker's false data injection is determined to maximize the system operation cost according to the decisions of the optimal economic dispatch. The decisions of the optimal economic dispatch are obtained by the solution of the lower level problem, which is the optimal economic dispatch optimization of the system operator with the contaminated measurements. The bi-level optimization model for the LR attack can be formulated as follows [12], [13].

$$\max_{\Delta\boldsymbol{P_L},\Delta\boldsymbol{P_F}} \sum_{g\in\mathcal{G}} c_g P_g^* + \sum_{l\in\mathcal{L}} c_l H_l^* \tag{1}$$

subject to

$$\sum_{l\in\mathcal{L}} \Delta P_l = 0 \tag{2}$$

$$\Delta\boldsymbol{P_F} = -\boldsymbol{SF}\cdot\boldsymbol{BL}\cdot\Delta\boldsymbol{P_L} \tag{3}$$

$$-\tau P_l \le \Delta P_l \le \tau P_l \quad \forall l\in\mathcal{L} \tag{4}$$

$$\left\{\boldsymbol{P}^*,\boldsymbol{H}^*\right\} = \arg\min_{\boldsymbol{P},\boldsymbol{H}} \left(\sum_{g\in\mathcal{G}} c_g P_g + \sum_{l\in\mathcal{L}} c_l H_l\right) \tag{5}$$

$$s.t. \quad \sum_{g\in\mathcal{G}} P_g = \sum_{l\in\mathcal{L}} (P_l - H_l) \tag{6}$$

$$\boldsymbol{P_F} = \boldsymbol{SF}\cdot\boldsymbol{BG}\cdot\boldsymbol{P_G} - \boldsymbol{SF}\cdot\boldsymbol{BL}\cdot(\boldsymbol{P_L}+\Delta\boldsymbol{P_L}-\boldsymbol{H_L}) \tag{7}$$

$$-P_f^{max} \le P_f \le P_f^{max} \quad \forall f\in\mathcal{F} \tag{8}$$

$$P_g^{min} \le P_g \le P_g^{max} \quad \forall g\in\mathcal{G} \tag{9}$$

$$0 \le H_l \le P_l + \Delta P_l \quad \forall l\in\mathcal{L} \tag{10}$$

where P_g is the generation dispatch of generator g, H_l is the load shedding of load l, c_g and c_l are the generation and load shedding costs per unit, τ is the maximum deviation rate of false data injections in load measurements, $\boldsymbol{SF}$ is the shifting factor matrix, $\boldsymbol{BG}$ is the bus-generation incidence matrix, $\boldsymbol{BL}$ is the bus-load incidence matrix, and $(-P_f^{max}, P_f^{max})$ and (P_g^{min}, P_g^{max}) are the capacity limits of the transmission lines and generation respectively. The objective of the attack model (1) is the system operation cost under the LR attack. The first term of (1) is the generation cost, and the second term is the load shedding cost. In the LR attack, a malicious attacker may aim to maximize the damage of the LR attack on the grid. The negative impacts of the LR attack are directly reflected on the increased system operation cost considering the load shedding due to the consequential dispatch decisions. Therefore, in the construction of the LR attack, (1) is applied as the objective [12], [13]. The operation of the grid is based on the results of the state estimation. As shown in the existing studies on the LR attack [12], [13], [19], if constraint (3) holds in the construction of the attack vector of the LR attack, the attacker is able to bypass the bad data detection and bury the injected data in the state estimation of the grid to mislead the system operator with the false state estimation. In the LR attack modeling, the DC power flow model is used. The DC power flow model is well accepted and commonly used in the economic dispatch of the power grid for its desirable simplicity, high robustness and fast convergence speed [19], [28], [29]. As the construction of the LR attack is based on the dispatch model, the DC power flow model of the grid is therefore used in the LR attack model. In the LR attack model above, it is assumed that the attacker is able to access the topology and measurement data of the grid to formulate the optimal attack strategy. The attacker may compromise the information and communication systems of the grid to obtain such data. Further, the difficulty of accessing the data is reduced considering the presence of the insider which has necessary knowledge and information of the grid. Therefore, following the works in [12], [13], this assumption is applied in the proposed model in this article.

In the LR attack, the attacker determines the attack vector to inject false data to the selected measurements, denoted by $\{\alpha_l, \alpha_f{:}\forall l\in\mathcal{L}, \forall f\in\mathcal{F}\}$. In the attack, it is not necessary for the attacker to manipulate the whole load and power flow measurements in the grid. Only part of the measurements in the grid are needed by the attacker to bypass the detection and formulate a valid attack. As shown in the case studies in this article and the results of a few existing works, e.g., [13], [16], the attacker can construct a damaging LR attack vector with limited contaminated measurements. As a countermeasure, the system operator (as the defender of the system) can strengthen the security of certain measurements to mitigate the damage. The strengthened protection on the measurement data security may include additional and more sophisticated encryption

and authentication schemes [30], [31], using redundant communication channels with tamper detection schemes [32], and methods combined [33]. The strengthened decision of the system operator is denoted by $\{\delta_l, \delta_f : \forall l \in \mathcal{L}, \forall f \in \mathcal{F}\}$. It is assumed that when the strengthened protection is performed on the measurement, this measurement cannot be compromised within the required time without being detected and false data cannot be injected to this measurement in the current attack attempt. Then we have the following constraints as (11).

$$\begin{aligned} &\Delta P_l = 0 \ \forall l \in \{l \in \mathcal{L} | \alpha_l = 0\} \cup \{l \in \mathcal{L} | \delta_l = 1\} \\ &\Delta P_f = 0 \ \forall f \in \left\{f \in \mathcal{F} | \alpha_f = 0\right\} \cup \left\{f \in \mathcal{F} | \delta_f = 1\right\} \end{aligned} \quad (11)$$

In order to integrate constraint (11) in the optimization in a closed form, it can be reformulated as follows.

$$-M\alpha_f \le \Delta P_f \le M\alpha_f \quad \forall f \in \mathcal{F} \quad (12)$$

$$-M\alpha_l \le \Delta P_l \le M\alpha_l \quad \forall l \in \mathcal{L} \quad (13)$$

$$-M\left(1-\delta_f\right) \le \Delta P_f \le M\left(1-\delta_f\right) \quad \forall f \in \mathcal{F} \quad (14)$$

$$-M(1-\delta_l) \le \Delta P_l \le M(1-\delta_l) \quad \forall l \in \mathcal{L} \quad (15)$$

Thus, the optimization model for the LR attack considering the attack and defense actions can be presented as (1) subject to (2)-(10) and (12)-(15). It is a bilevel optimization problem which can be solved with the penalized function based method [34] or the Karush-Kuhn-Tucker (KKT) conditions based method by reformulating the original model into a single-level optimization problem [12].

B. Security Resource Allocation Game Modeling of Load Redistribution Attacks

In the LR attack model, both the system operator and attacker need to consider each other's strategies in order to obtain the optimal payoffs. In this case, the LR attack problem can be formulated as a security resource allocation game model. In cybersecurity, it has been increasingly realized that the misunderstanding on the incentives of the involved entities rather than the lack of proper technical mechanisms is more likely to cause the security failures in the information systems [35]. Therefore, game theoretic models have been extensively applied to the cybersecurity research as the game theory provides a proper framework to systematically reason about the behaviors of the defender and attacker, and facilitates the design of efficient defense strategies. With the solution of the game models, the optimal strategies of the defender and attacker against each other can be obtained. Thus, the game theory based model is applied in this study. In the proposed game model, it is assumed that both the defender and attacker are rational. In other words, both of them will apply the best response to the strategy of the opponent to optimize his/her own payoff in the game, which is a rational and well accepted assumption in the game theoretic studies.

1) System Operator's Model: As the defender in the game, the system operator aims to minimize the system operation cost in the attack. Thus, the payoff function of the defender is defined as the negative of the system operation cost according to the optimal economic dispatch with the contaminated measurements in the LR attack. It is presented as follows.

$$U_{\mathcal{D}} = -\left(\sum_{g\in\mathcal{G}} c_g P_g^* + \sum_{l\in\mathcal{L}} c_l H_l^*\right) \quad (16)$$

The strategy of the defender is denoted by $s_{\mathcal{D}} = \{\delta_l, \delta_f : \forall l \in \mathcal{L}, \forall f \in \mathcal{F}\}$. The defense strategies are constrained by the defender's resource limit $R_{\mathcal{D}}$.

$$\sum_{l\in\mathcal{L}} \kappa_l \delta_l + \sum_{f\in\mathcal{F}} \kappa_f \delta_f \le R_{\mathcal{D}} \quad (17)$$

where κ_l and κ_f are the costs of the strengthened actions.

2) Attacker's Model: In the LR attack, the attacker aims to maximize the system operation cost. Therefore, the payoff function of the attacker is the negative of the defender's payoff. It is presented as follows.

$$U_{\mathcal{A}} = -U_{\mathcal{D}} = \sum_{g\in\mathcal{G}} c_g P_g^* + \sum_{l\in\mathcal{L}} c_l H_l^* \quad (18)$$

The strategy of the attacker is denoted by $s_{\mathcal{A}} = \{\alpha_l, \alpha_f : \forall l \in \mathcal{L}, \forall f \in \mathcal{F}\}$. The attack strategies are constrained by the attacker's resource limit $R_{\mathcal{A}}$.

$$\sum_{l\in\mathcal{L}} \nu_l \alpha_l + 2\sum_{f\in\mathcal{F}} \nu_f \alpha_f \le R_{\mathcal{A}} \quad (19)$$

where ν_l and ν_f are the costs of the attack actions. When the system is fully measured, the attacker needs to compromise the measurements in both directions of a transmission line in order to inject false data to the power flow measurement [12]. Thus, the resources spent by the attack actions on the power flow measurements are doubled in constraint (19).

3) Mixed Strategy Nash Equilibrium: Generally, it is not necessarily true that a pure strategy Nash Equilibrium must exist in a security game. However, with finite action spaces of the players, the mixed-strategy Nash Equilibrium exists in the security resource allocation game. We denote the set of the defender's pure strategies by $\mathbf{S}_{\mathcal{D}}$ and the cardinal number of $\mathbf{S}_{\mathcal{D}}$ by $N_{\mathcal{D}}$. Similarly, the set of the attacker's pure strategies is denoted by $\mathbf{S}_{\mathcal{A}}$, and the cardinal number of $\mathbf{S}_{\mathcal{A}}$ is denoted by $N_{\mathcal{A}}$. The mixed strategy of a player in the game is the probability profile of the player choosing any of his/her pure strategies. Thus, we can further denote the mixed strategy of the defender by $\pi_{\mathcal{D}} = \{\pi_1, \pi_2, \ldots, \pi_{N_{\mathcal{D}}}\}$ in which π_i is the probability of the defender adopting the pure defense strategy $s_{\mathcal{D}i} \in \mathbf{S}_{\mathcal{D}}$, $i \in \{1, 2, \ldots, N_{\mathcal{D}}\}$. Likewise, we denote the mixed strategy of the attacker by $\varpi_{\mathcal{A}} = \{\varpi_1, \varpi_2, \ldots, \varpi_{N_{\mathcal{A}}}\}$ in which ϖ_j is the probability of the attacker adopting the pure attack strategy $s_{\mathcal{A}j} \in \mathbf{S}_{\mathcal{A}}$, $j \in \{1, 2, \ldots, N_{\mathcal{A}}\}$. Considering the probabilities of all possible pure strategies, the constraint for the defender and attacker's mixed strategies is as follows.

$$\sum_{i=1}^{N_{\mathcal{D}}} \pi_i = 1, \sum_{j=1}^{N_{\mathcal{A}}} \varpi_j = 1 \quad (20)$$

At the mixed strategy Nash equilibrium of the game, neither the defender nor the attacker can increase his/her payoff by

unilaterally altering his/her strategy. Hence:

$$\overline{U}_{\mathcal{D}}(\pi^*_{\mathcal{D}}, \varpi^*_{\mathcal{A}}) \geq \overline{U}_{\mathcal{D}}(\pi'_{\mathcal{D}}, \varpi^*_{\mathcal{A}}),$$
$$\overline{U}_{\mathcal{A}}(\pi^*_{\mathcal{D}}, \varpi^*_{\mathcal{A}}) \geq \overline{U}_{\mathcal{A}}(\pi^*_{\mathcal{D}}, \varpi'_{\mathcal{A}}) \tag{21}$$

where π^*_D and ϖ^*_A are the defender and attacker's mixed strategies at Nash Equilibrium respectively, π'_D and ϖ'_A are the deviant strategies of the defender and attacker. The expected payoffs of the defender and attacker with the mixed strategies can be calculated as (22) and (23), respectively.

$$\overline{U}_{\mathcal{D}} = -\sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\pi_i\varpi_j\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right) \tag{22}$$

$$\overline{U}_{\mathcal{A}} = \sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\pi_i\varpi_j\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right) \tag{23}$$

where $P^*_{g,\mathcal{D}i,\mathcal{A}j}$ and $H^*_{l,\mathcal{D}i,\mathcal{A}j}$ are the optimal solutions of the lower level problem (5)-(10) in the LR attack model when the defense strategy $s_{\mathcal{D}} = s_{\mathcal{D}i}$ and the attack strategy $s_{\mathcal{A}} = s_{\mathcal{A}j}$.

III. Insider Threats in Load Redistribution Attacks

In the presence of insider threats, there is a chance that the instantiation of the defender's mixed strategy will be leaked to the attacker in the attacks. Such information leakage will give the attacker great advantages in the game and increase the damage of the LR attacks. In this section, the detailed formulation of the information leakage will be developed and the mixed strategy Nash Equilibrium of the security game with insider threats will be calculated.

In this study, it is assumed that there is a probability that the insider will expose the protection status in a subset of the measurements in the instantiation of the mixed defense strategy to the attacker. In cybersecurity, information leakage is an important issue. For the reasons as discussed in Section I, the insider may be complicit in the attack with the attacker. Thus, following the work in [27], the possibility of partial exposure of the protection status is assumed in the proposed model in this article.

Let $\mathcal{M}$ be a subset of the measurements in the security game ($\mathcal{M} \subseteq \mathcal{L} \bigcup \mathcal{F}$). Suppose with probability p_0 ($0 \leq p_0 \leq 1$) the instantiation of the protection status $\hat{\delta} = \{\hat{\delta}_m, \forall m \in \mathcal{M}\}$ is leaked by the insider. The probability p_0 and the size of the information leakage set $\mathcal{M}$ reflect the ability of the insider. When the instantiation is leaked to the attacker, the attacker can predict the defender's action more accurately. The action space of the defender is reduced to a smaller subset of the original space. In this subspace of defense actions, the pure strategies in set $\mathcal{M}$ are certain, which should be identical to the leaked instantiation $\hat{\delta}$. With the additional information, the attacker can adjust his/her mixed strategy to improve the payoff. We denote the mixed strategy of the attacker by $\varpi_{\hat{\delta}} = \{\varpi_{\hat{\delta},1}, \varpi_{\hat{\delta},2}, \ldots, \varpi_{\hat{\delta},N_{\mathcal{A}}}\}$ when the instantiation of the defender's mixed strategy $\hat{\delta}$ is leaked. Then, the expected payoff of the attacker can be formulated as (24) when the instantiation of the defender's mixed strategy is leaked by the insider.

$$\overline{U}_{\mathcal{A}} = \sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\mathbf{Pr}\Big(s_{\mathcal{D}i} \mid \delta_m = \hat{\delta}_m, \forall m \in \mathcal{M}\Big)\cdot\varpi_{\hat{\delta},j} \times\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right) \tag{24}$$

The conditional probabilities $\mathbf{Pr}(s_{\mathcal{D}i} \mid \delta_m = \hat{\delta}_m, \forall m \in \mathcal{M})$ are the probability profile of the defender's strategy on condition that the defense actions in set $\mathcal{M}$ are exactly the same as the exposed instantiation $\hat{\delta}_m, \forall m \in \mathcal{M}$. They can be determined by the mixed strategy of the defender as follows.

$$\mathbf{Pr}\Big(s_{\mathcal{D}i} \mid \delta_m = \hat{\delta}_m, \forall m \in \mathcal{M}\Big) = \frac{k_i\pi_i}{\sum_{i=1}^{N_{\mathcal{D}}} k_i\pi_i} \tag{25}$$

where

$$k_i = \begin{cases} 1, & \text{if } \delta_m = \hat{\delta}_m,\ \delta_m \in s_{\mathcal{D}i}, \forall m \in \mathcal{M} \\ 0, & \text{otherwise} \end{cases} \tag{26}$$

When the instantiation of the defender's mixed strategy is not exposed, the case is identical to the original security game model. In this case, the expected payoff of the attacker is calculated by (23). Hence, when the defense strategy instantiation is $\hat{\delta}$, the expected payoff function of the attacker can be formulated as (27).

$$\begin{aligned}\overline{U}_{\mathcal{A}} = {} & (1-p_0)\sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\pi_i\varpi_j\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right) \\ & + p_0\sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\mathbf{Pr}\Big(s_{\mathcal{D}i} \mid \delta_m = \hat{\delta}_m, \forall m \in \mathcal{M}\Big)\varpi_{\hat{\delta},j} \\ & \times\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right) - \eta C_{in}(p_0, \mathcal{M})\end{aligned} \tag{27}$$

where C_{in} is the cost for the information leakage to the insider, and η is the cost coefficient of the attacker. The first term in (27) is the expected payoff of the attacker when the instantiation of the defender's mixed strategy is not exposed. The second term is the expected payoff when the information about the defender's strategy is leaked. The third term is the cost of the attacker to obtain the information from the insider. Then the expected payoff function of the defender can likewise be formulated as (28) when the defense strategy instantiation is $\hat{\delta}$.

$$\begin{aligned}\overline{U}_{\mathcal{D}} = {} & (p_0-1)\sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\pi_i\varpi_j\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right) \\ & - p_0\sum_{i=1}^{N_{\mathcal{D}}}\sum_{j=1}^{N_{\mathcal{A}}}\mathbf{Pr}\Big(s_{\mathcal{D}i} \mid \delta_m = \hat{\delta}_m, \forall m \in \mathcal{M}\Big)\varpi_{\hat{\delta},j} \\ & \times\left(\sum_{g\in\mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l\in\mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j}\right)\end{aligned} \tag{28}$$

In general, the information leakage probability p_0 and the information leakage set $\mathcal{M}$ of the insider are determined when

the LR attack is performed. Hence, the term for the payment to the insider by the attacker in (27) can be considered constant and neglected in the model. Then,

$$\overline{U}_{\mathcal{D}} = -\overline{U}_{\mathcal{A}} \tag{29}$$

In this case, the model between the system operator and attacker becomes a zero-sum game. Hence, a mixed strategy Nash Equilibrium of the game is guaranteed. Considering that the probability of the presence of observation $\hat{\delta}$ is $\sum_{i=1}^{N_{\mathcal{D}}} k_i \pi_i$, the expected payoffs of the attacker and system operator can be derived as (30) and (31) respectively by summing up the expected payoffs of all possible observations $\hat{\delta}$ weighted by the probabilities.

$$\begin{aligned}\overline{U}_{\mathcal{A}} = {} & (1-p_0) \sum_{i=1}^{N_{\mathcal{D}}} \sum_{j=1}^{N_{\mathcal{A}}} \pi_i \varpi_j \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \\ & + p_0 \sum_{\hat{\delta} \in \hat{\Delta}} \sum_{i=1}^{N_{\mathcal{D}}} \sum_{j=1}^{N_{\mathcal{A}}} k_i \pi_i \varpi_{\hat{\delta},j} \\ & \times \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \end{aligned} \tag{30}$$

$$\begin{aligned}\overline{U}_{\mathcal{D}} = {} & -\overline{U}_{\mathcal{A}} \\ = {} & (p_0 - 1) \sum_{i=1}^{N_{\mathcal{D}}} \sum_{j=1}^{N_{\mathcal{A}}} \pi_i \varpi_j \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \\ & - p_0 \sum_{\hat{\delta} \in \hat{\Delta}} \sum_{i=1}^{N_{\mathcal{D}}} \sum_{j=1}^{N_{\mathcal{A}}} k_i \pi_i \varpi_{\hat{\delta},j} \\ & \times \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \end{aligned} \tag{31}$$

where $\hat{\Delta}$ is the set of all the possible instantiation observation by the insider. With the above formulation of the payoffs in the zero-sum game model, the mixed strategies of the attacker and system operator at the Nash Equilibrium of the game can be formulated as the minimax problem and solved efficiently. For the attacker, the optimal mixed strategy is to maximize the minimum of $\overline{U}_{\mathcal{A}}$ with all the system operator's pure strategies because the objective of the system operator is actually to minimize $\overline{U}_{\mathcal{A}}$. Hence, it can be formulated and solved as follows.

$$\max_{\varpi_j, \varpi_{\hat{\delta},j}} \ \overline{U}_{\mathcal{A}} \tag{32}$$

subject to

$$\overline{U}_{\mathcal{A}} \le U_i \quad \forall i \in \{1, 2, \ldots, N_{\mathcal{D}}\} \tag{33}$$

$$\begin{aligned} U_i = {} & (1-p_0) \sum_{j=1}^{N_{\mathcal{A}}} \varpi_j \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \\ & + p_0 \sum_{\hat{\delta} \in \hat{\Delta}} \sum_{j=1}^{N_{\mathcal{A}}} k_i \varpi_{\hat{\delta},j} \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \\ & \forall i \in \{1, 2, \ldots, N_{\mathcal{D}}\} \end{aligned} \tag{34}$$

$$\sum_{j=1}^{N_{\mathcal{A}}} \varpi_j = 1 \tag{35}$$

$$0 \le \varpi_j \le 1 \quad \forall j \in \{1, 2, \ldots, N_{\mathcal{A}}\} \tag{36}$$

$$\sum_{j=1}^{N_{\mathcal{A}}} \varpi_{\hat{\delta},j} = 1 \quad \forall \hat{\delta} \in \hat{\Delta} \tag{37}$$

$$0 \le \varpi_{\hat{\delta},j} \le 1 \quad \forall \hat{\delta} \in \hat{\Delta},\ \forall j \in \{1, 2, \ldots, N_{\mathcal{A}}\} \tag{38}$$

For the system operator, the mixed strategy is to minimize the maximum of $\overline{U}_{\mathcal{A}} = -\overline{U}_{\mathcal{D}}$ with all the attacker's pure strategies because of the opposite objective of the attacker. Hence, it can be formulated and solved as follows.

$$\min_{\pi_i} \ -\overline{U}_{\mathcal{D}} \tag{39}$$

subject to

$$-\overline{U}_{\mathcal{D}} = U_0 + \sum_{\hat{\delta} \in \hat{\Delta}} U_{\hat{\delta}} \tag{40}$$

$$U_0 \ge U_j \quad \forall j \in \{1, 2, \ldots, N_{\mathcal{A}}\} \tag{41}$$

$$U_{\hat{\delta}} \ge U_{\hat{\delta},j} \quad \forall \hat{\delta} \in \hat{\Delta},\ \forall j \in \{1, 2, \ldots, N_{\mathcal{A}}\} \tag{42}$$

$$\begin{aligned} U_j = {} & (1-p_0) \sum_{i=1}^{N_{\mathcal{D}}} \pi_i \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \\ & \forall j \in \{1, 2, \ldots, N_{\mathcal{A}}\} \end{aligned} \tag{43}$$

$$\begin{aligned} U_{\hat{\delta},j} = {} & p_0 \sum_{i=1}^{N_{\mathcal{D}}} k_i \pi_i \left(\sum_{g \in \mathcal{G}} c_g P^*_{g,\mathcal{D}i,\mathcal{A}j} + \sum_{l \in \mathcal{L}} c_l H^*_{l,\mathcal{D}i,\mathcal{A}j} \right) \\ & \forall \hat{\delta} \in \hat{\Delta},\ \forall j \in \{1, 2, \ldots, N_{\mathcal{A}}\} \end{aligned} \tag{44}$$

$$\sum_{i=1}^{N_{\mathcal{D}}} \pi_i = 1 \tag{45}$$

$$0 \le \pi_j \le 1 \quad \forall i \in \{1, 2, \ldots, N_{\mathcal{D}}\} \tag{46}$$

In the LR attack model, the values of the operation cost of the system and the corresponding dispatch decisions P^*_g and H^*_l with the manipulated measurements can be determined by the solution of the optimization model (1) subject to (2)-(10) and (12)-(15). As shown in constraints (12)-(15), the manipulated measurements are constrained by both the attack and protection actions. Therefore, against the LR attack, the defender may perform the protection actions on the load and power flow measurements in the grid according to the mixed defense strategy obtained by optimizing the payoff of the defender as (22) without considering the insider threat. However, due to the presence of the insider, the instantiation of the protection actions in a set of measurements may be exposed to the attacker. With the exposed protection status, the attacker can determine the mixed strategy of the LR attack ϖ_j and $\varpi_{\hat{\delta},j}$ according to the solution of the optimization model as (32)-(38). Then, the attacker can perform the attack actions α_l and α_f on the measurements in the grid according to the obtained mixed attack strategy. When noticing the presence of the insider threat, the defender may update the mixed defense strategy with the proposed optimization model as (39)-(46) to achieve the best response against the strategy of the attacker with the insider threat. Then the protection actions can be

performed by the defender according to the updated mixed defense strategy which considers the information leakage of the defense strategy. In the proposed game model, the attacker and defender need to know or estimate the action space of his/her opponent, which includes the load and power flow measurements in the grid in this study. Then, as the players in the game, both the attacker and defender are assumed to be rational and will optimize his/her own payoff in the game considering the response of the opponent to the strategy. Thus, in the models of the attacker and defender, the action of the opponent can be expected and can be formulated by optimizing the corresponding payoff.

It should be noted that the increase of the number of the security resources will improve the payoff of the defender. When the number of the security resources increases, the damage of the LR attack with or without insider threats will decrease (at least be the same as the original case), and correspondingly the payoff of the attacker will decrease. It is because with more security resources, the defender can cover and secure more measurements in the grid. Consequently, it is more difficult for the attacker to construct valid attack vectors. In the proposed model, when the number of the security resources increases, the defense strategy at the original case will become the solution over a subset of the feasible set in the defender model given any attack strategy of the attacker. As a result, it is a sub-optimal solution for the defender, and the payoff of the defender will be improved (at least be the same as the original case) when the number of the security resources increases. Thus, in the proposed model, the defender will always use up all the available security resources to secure the grid, and a higher number of security resources always benefits the defender.

IV. Case Studies

Case studies were carried out to demonstrate the proposed security resource allocation game model of the LR attack considering the information leakage as well as study the impacts of the insider threats to the payoffs of the system operator and attacker in the attack. The details of the case studies are described in this section.

A. Parameters in Case Studies

In the case studies, scenarios were simulated on the modified IEEE 39-bus system. The single line diagram of the system is shown in Fig. 1.

The generation costs and capacities of the generators in the power system are listed in Table I, and the lower output limit P_g^{min} is zero for all the generators. Other parameters in the simulations are listed in Table II.

In the case studies, the optimization models were solved using CPLEX on a laptop with Intel Core i5 CPU (1.60-3.90GHz) and 12GB RAM.

B. Case Study Results

When there is no attack on the power system, the system is operated in the optimal operation state according to the optimal economic dispatch determined by the system operator.

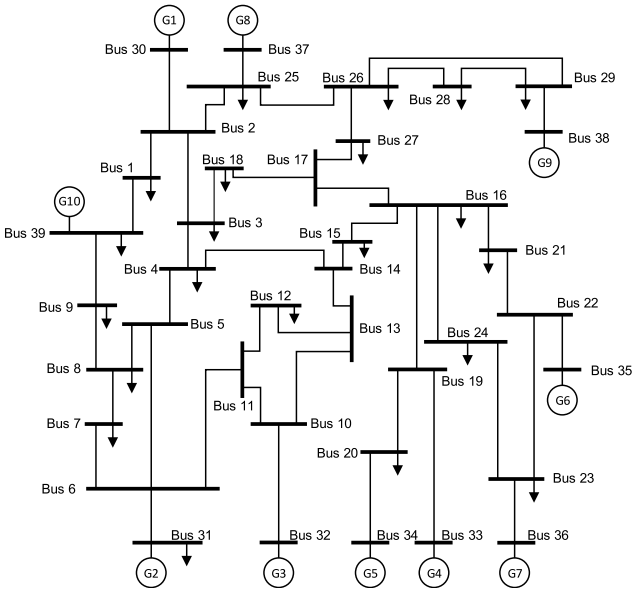


Fig. 1. IEEE 39-bus Test System.

TABLE I
Costs & Capacities of Generators

Generator No.	**G1**	**G2**	**G3**	**G4**	**G5**
P_g^{max} (MW)	1040	646	725	652	508
c_g ($/MWh)	5	10	10	10	20
Generator No.	**G6**	**G7**	**G8**	**G9**	**G10**
P_g^{max} (MW)	687	580	564	865	1100
c_g ($/MWh)	50	10	20	10	5

TABLE II
Key Parameters in Case Studies

Parameter	**Value**
Load Shedding Cost (c_l)	200 $/MWh
Information Leakage Probability (p_0)	0.8
Measurement Deviation Limit (τ)	0.2
Resource Cost of Attack Action (ν_l, ν_f)	1
Attack Resource Limit ($R_{\mathcal{A}}$)	10
Resource Cost of Defense Action (κ_l, κ_f)	1
Defense Resource Limit ($R_{\mathcal{D}}$)	3

TABLE III
Optimal Attack Vector

Attacked Load Measurement No.	ΔP_l (MW)	**Attacked Flow Measurement No.**	ΔP_f (MW)
Bus 1	99.52	Line 1-39	-99.52
Bus 8	40.59	Line 8-9	-40.59
Bus 39	-140.11	Line 9-39	-40.59

The optimal operation cost of the system is $67,100.23, and no load shedding is needed in this case.

In the base case with the LR attack, it is assumed that no defense actions are taken by the system operator. The attacker selects the optimal attack vector to maximize the operation cost of the system. The optimal vector for the attacker is listed in Table III.

With the contaminated measurements, the outputs of the generators are re-dispatched by the operator, and meanwhile a

TABLE IV
MIXED STRATEGY OF ATTACKER WITHOUT INFORMATION LEAKAGE

Mixed Strategy	Attack Vector
0.169	Bus 1, Bus 3, Bus 4, Bus 16, Bus 20, Line 16-19, Line 19-20
0.452	Bus 26, Bus 28, Bus 29, Line 26-28, Line 26-29, Line 28-29
0.115	Bus 1, Bus 8, Bus 9, Bus 39, Line 1-39, Line 8-9, Line 9-39
0.263	Bus 16, Bus 21, Bus 23, Bus 24, Line 16-21, Line 16-23, Line 23-24

TABLE V
MIXED STRATEGY OF SYSTEM OPERATOR WITHOUT INFORMATION LEAKAGE

Mixed Strategy	Measurement Protection Selection
0.104	Bus 8, Bus 21, Line 26-29
0.319	Bus 8, Bus 26, Line 26-29
0.179	Bus 16, Bus 26, Line 26-29
0.009	Bus 21, Bus 26, Line 28-29
0.388	Line 8-9, Line 16-19, Line 16-21

total of about 137 MW of load at Buses 1, 7 and 8 is shed in this case. As a result, the operation cost of the system increases dramatically to $94,007.58.

When the defense actions are taken by the system operator, a mixed strategy Nash equilibrium is achieved when both the system operator and attacker's actions are the best decisions to maximize their payoffs. In the case when no insider exists, the mixed strategies of the system operator and attacker are shown in Table IV and Table V, respectively. The optimal strategies of both the system operator and attacker with the proposed model are identical with the best response of the system operator and attacker to each other's strategies. In other words, the proposed model provides the best strategies of both the system operator and attacker considering each other's actions in the game.

The expected operation cost of the system is $72,179.18 in this case. Although the expected operation cost is still higher than the original case when there is no attack to the system, the defense strategy of the system operator greatly decreases the operation cost under the LR attack even if the defense resource is limited. The strategies of the attacker and defender at the Nash equilibrium of the game provide the best response to each other's actions. Therefore, it is the optimal solution considering the strategy of the opponent, and either player has no incentive to change his/her strategy. Thus, the damage of the attack will be reduced if the attacker simply chooses a random attack strategy. Fig. 2 shows the comparison between the results at the Nash Equilibrium of the game and when the attacker applies a random attack strategy over the support of its mixed strategy. As shown in the figure, if the attacker applies the random attack strategy, the expected system cost will be reduced from $72,179.18 to $70,090.58 when the system operator keeps the defense strategy at the Nash equilibrium. The number will further decrease to $68,551.07 if the system operator applies the optimal defense strategy against the random attack strategy.

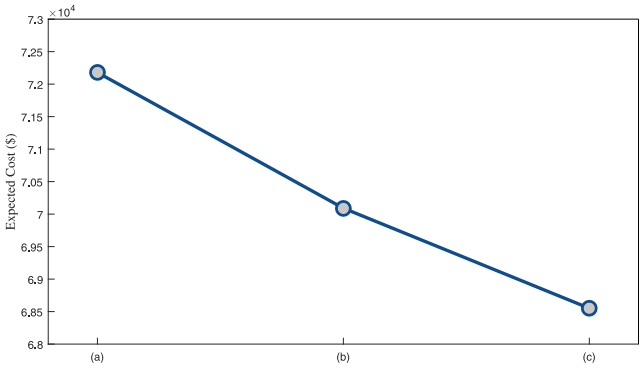


Fig. 2. Comparison between Results (a) at Nash Equilibrium, (b) with Defense Strategy at Nash Equilibrium under Random Attack Strategy, and (c) with Optimal Defense Strategy against Random Attack Strategy.

TABLE VI
ATTACK ACTIONS OF ATTACKER

Protection Status	Attack Vector
$\delta_{Bus26} = 1$	Bus 16, Bus 21, Bus 23, Bus 24, Line 16-21, Line 16-23, Line 23-24
$\delta_{Bus26} = 0$	Bus 26, Bus 28, Bus 29, Line 26-28, Line 26-29, Line 28-29

TABLE VII
MIXED STRATEGY OF SYSTEM OPERATOR WITH INFORMATION LEAKAGE

Mixed Strategy	Measurement Protection Selection
0.119	Bus 8, Bus 16, Bus 27
0.287	Bus 8, Bus 20, Bus 21
0.109	Bus 8, Bus 21, Line 26-29
0.288	Bus 8, Line 26-28, Line 28-29
0.141	Bus 16, Line 26-28, Line 28-29
0.057	Bus 21, Bus 28, Bus 29

However, when the insider exists and the information of the defense strategy is leaked to the attacker, the expected operation cost of the system increases. In this scenario, it is assumed that the protection status of the load measurement at Bus 26 is leaked by the insider to the attacker with a probability $p_0 = 0.8$. If the system operator does not realize the existence of the insider and keeps the original strategy, the attacker will also remain the original mixed strategy for attack actions when the defense strategy instantiation is not leaked. Nevertheless, when the defense strategy instantiation of the load measurement at Bus 26 is exposed, the attacker will change the attack actions to take advantages of the information leakage. The actions of the attacker dependent on the observation of the protection status of the load measurement at Bus 26 when the information is exposed, which are listed in Table VI. In doing so, the attacker increases the expected operation cost of the system to $76,256.80.

On the contrary, if the system operator realizes the existence of insider threats and the probability of information leakage, the system operator is able to change its mixed strategy to reduce the expected operation cost of the system under the LR attack with the information leakage. The mixed strategy of the system operator is listed in Table VII.

TABLE VIII
MIXED STRATEGY OF ATTACKER WITH INFORMATION LEAKAGE

Mixed Strategy		Attack Vector
Not leaked	1	Bus 26, Bus 28, Bus 29, Line 26-28, Line 26-29, Line 28-29
Instantiation leaked: $\delta_{Bus26} = 1$	0.373	Bus 16, Bus 20, Line 16-19, Line 19-20
	0.241	Bus 28, Bus 29, Line 26-28, Line 26-29, Line 28-29
	0.193	Bus 1, Bus 8, Bus 9, Bus 39, Line 1-39, Line 8-9, Line 9-39
	0.193	Bus 16, Bus 21, Bus 23, Bus 24, Line 16-21, Line 16-23, Line 23-24
Instantiation leaked: $\delta_{Bus26} = 0$	0.159	Bus 16, Bus 20, Line 16-19, Line 19-20
	0.310	Bus 1, Bus 3, Bus 25, Bus 26, Bus 27, Line 25-26, Line 26-27
	0.175	Bus 26, Bus 28, Bus 29, Line 26-28, Line 26-29, Line 28-29
	0.108	Bus 1, Bus 8, Bus 9, Bus 39, Line 1-39, Line 8-9, Line 9-39
	0.248	Bus 16, Bus 21, Bus 23, Bus 24, Line 16-21, Line 16-23, Line 23-24

Meanwhile, the attacker will change the mixed strategy for the attack action according to the information leakage status to maximize the expected operation cost of the system. The mixed strategies of the attacker are listed in Table VIII.

With the changes of the mixed strategies taken by the system operator and attacker, the expected operation cost of the system is reduced to \$72,416.23 consequently. As the system operator realizes the probability of information leakage by the insider, the defense strategy is changed to respond to the attack actions optimally and limit the potential damage to the system by the attacker's strategies. Thus, the expected operation cost of the system is reduced compared to the case where the existence of the insider is not realized by the system operator.

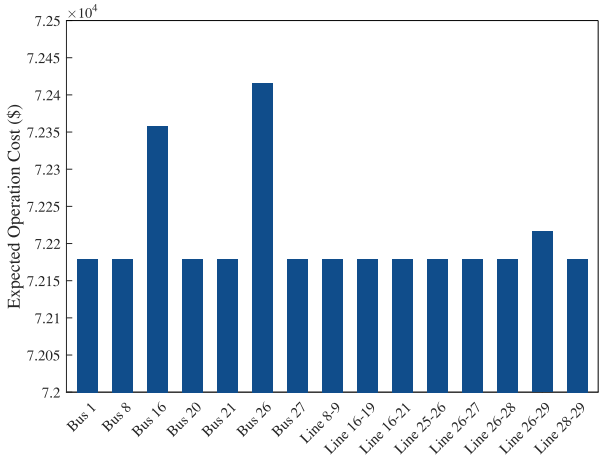


Fig. 3. Expected Operation Costs to Leaked Protection Status of Measurements.

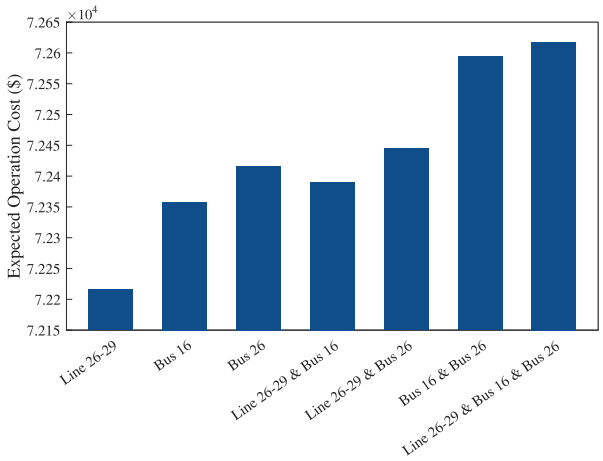


Fig. 4. Expected Operation Costs with Different Information Leakage Sets.

C. Impact of Information Leakage Set

The composition of the set of measurements $\mathcal{M}$ whose protection instantiation may be leaked by the insider has great impacts on the potential damage of the LR attack. Fig. 3 shows the expected operation costs of the system in the cases of each individual measurement may be leaked by the insider. The leakage probability $p_0 = 0.8$. As shown in the figure, the information leakage of a series of measurements will not increase the damage of the LR attack. However, the leakage of the protection status of a few critical measurements in the grid will raise the expected operation cost of the system, i.e., the payoff of the attacker. With the simulations on the proposed game model considering the insider threat, these critical measurements in the grid can be identified. In this case, the critical measurements include Bus 16, Bus 26, and Line 26-29.

Further, the size of the information leakage set $\mathcal{M}$ will also influence the potential damage of the LR attack with information leakage through the insider. Fig. 4 shows the expected operation costs of the system when set $\mathcal{M}$ is the non-empty subset of {Bus 16, Bus 26, Line 26-29}. As shown in the figure, the expected operation cost of the system rises with the size of set $\mathcal{M}$ in general.

D. Impact of Leakage Probability

Besides the composition and size of the information leakage set $\mathcal{M}$, the value of the information leakage probability p_0 will impact the potential damage of the LR attack as well. The expected operation costs of the system in the LR attack to the leakage probability p_0 are shown in Fig. 5. The figure shows the cases when the protection status of measurement of Bus 16, Bus 26 or Line 26-29 may be exposed by the insider. Not surprisingly, the expected operation costs of the system increase with the increase of the leakage probability p_0. More importantly, the expected operation costs of the system increase rapidly in the low value area and reaches the plateau when p_0 is still small. As shown by the curves in Fig. 5, the expected operation costs of the system in all the cases are already close to the maximums when p_0 is only about 30%. Thus, even if the information leakage probability is small, the potential damage of the information leakage in the LR attack can be considerable to the system. The information leakage from the insider is of great value to the attacker to enhance his/her payoff in the LR attack.

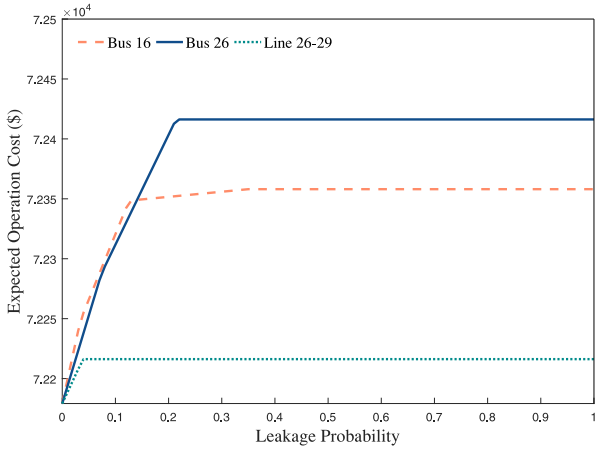


Fig. 5. Expected Operation Costs to Information Leakage Probability.

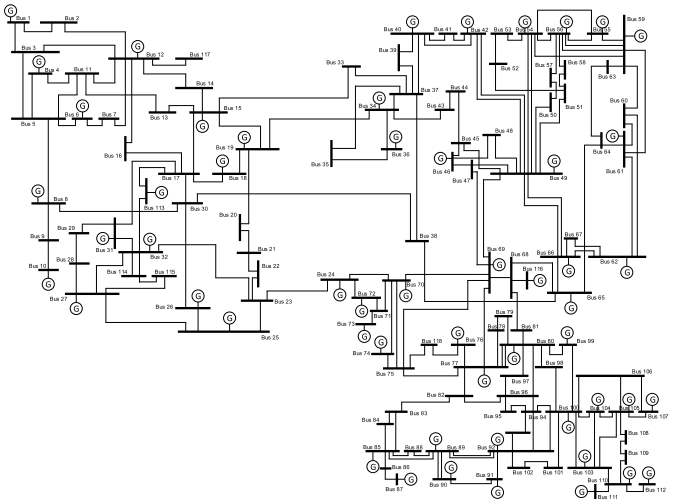


Fig. 6. IEEE 118-bus Test System.

E. Case Study on IEEE 118-Bus System

In order to further validate the proposed model of the LR attack on power systems considering the insider threats, a case study was also conducted on the IEEE 118-bus system. The single line diagram of the system is shown in Fig. 6. The parameters of the proposed model in the simulation remained the same as those in the previous cases on the IEEE 39-bus system as listed in Table II.

In the case when there is no insider threat, the mixed strategies of the attacker and system operator at the Nash equilibrium are shown in Table IX and Table X, respectively. With the defense actions of the system operator, the expected increased operation cost of the system is about $1213.24. However, similar to the previous cases on the IEEE 39-bus system, when the information leakage due to the insider exists, the game is changed. In this scenario, it is assumed that the protection status of the load measurement at Bus 77 may be exposed to the attacker with a probability $p_0 = 0.8$ due to the insider threat. If the system operator does not realize the existence of the information leakage and keeps the original strategy, the attacker will remain the original mixed attack strategy when the defense strategy instantiation is not leaked. However, when the protection instantiation of the load measurement at Bus 77 is exposed, the attacker may adjust the attack actions according to the observation of the protection status as listed in Table XI. As a result, the expected increased operation cost of the system rises significantly to about $2183.83, which is an about 80% raise compared with the original case without the insider.

However, if the system operator realizes the existence of the insider threat and information leakage, the system operator may change the mixed strategy of the defense to reduce the cost. The mixed strategy of the system operator is listed in Table XII. Meanwhile, the attacker may adjust the mixed strategies of the attack according to the information leakage status to maximize the system operation cost as listed in Table XIII. In this case, the expected increased operation cost of the system due to the LR attack drops to $1362.13, which is markedly lower than the case when the information leakage is not considered in the model of the system operator.

TABLE IX
MIXED STRATEGY OF ATTACKER WITHOUT INFORMATION LEAKAGE ON 118-BUS SYSTEM

Mixed Strategy	Attack Vector
0.071	Bus 1, Bus 2, Bus 3, Line 1-2, Line 1-3, Line 3-5
0.234	Bus 11, Bus 13, Bus 15, Bus 19, Line 11-13, Line 13-15, Line 15-19
0.231	Bus 19, Bus 33, Bus 34, Bus 35, Line 19-34, Line 34-36, Line 35-36
0.177	Bus 40, Bus 41, Bus 42, Line 40-41, Line 40-42, Line 41-42
0.088	Bus 54, Bus 55, Bus 56, Bus 59, Line 54-55, Line 55-56, Line 55-59
0.099	Bus 75, Bus 76, Bus 77, Bus 118, Line 75-77, Line 76-77, Line 76-118
0.101	Bus 78, Bus 79, Bus 80, Line 78-79, Line 79-80, Line 80-81

TABLE X
MIXED STRATEGY OF SYSTEM OPERATOR WITHOUT INFORMATION LEAKAGE ON 118-BUS SYSTEM

Mixed Strategy	Measurement Protection Selection
0.313	Bus 3, Bus 77, Bus 80
0.065	Bus 15, Bus 54, Line 1-2
0.076	Bus 36, Bus 54, Line 1-2
0.252	Bus 40, Bus 54, Line 1-2
0.009	Bus 54, Bus 77, Line 1-2
0.243	Bus 55, Bus 77, Bus 80
0.041	Bus 77, Bus 99, Line 9-10

TABLE XI
ATTACK ACTIONS OF ATTACKER ON 118-BUS SYSTEM

Protection Status	Attack Vector
$\delta_{Bus77} = 1$	Bus 1, Bus 2, Bus 3, Line 1-2, Line 1-3, Line 3-5
$\delta_{Bus77} = 0$	Bus 75, Bus 76, Bus 77, Bus 118, Line 75-77, Line 76-77, Line 76-118

TABLE XII
MIXED STRATEGY OF SYSTEM OPERATOR WITH INFORMATION LEAKAGE ON 118-BUS SYSTEM

Mixed Strategy	Measurement Protection Selection
0.346	Bus 3, Bus 76, Bus 79
0.107	Bus 41, Bus 54, Bus 79
0.099	Bus 54, Bus 76, Line 21-22
0.043	Bus 54, Bus 79, Bus 118
0.335	Bus 54, Bus 96, Line 1-2
0.018	Bus 54, Bus 118, Line 35-36
0.051	Bus 79, Bus 96, Bus 118

TABLE XIII
MIXED STRATEGY OF ATTACKER WITH INFORMATION LEAKAGE ON 118-BUS SYSTEM

Mixed Strategy		Attack Vector
Not leaked	1	Bus 1, Bus 2, Bus 3, Line 1-2, Line 1-3, Line 3-5
Instantiation leaked: $\delta_{Bus77} = 1$	0.141	Bus 1, Bus 2, Bus 3, Line 1-2, Line 1-3, Line 3-5
	0.351	Bus 40, Bus 41, Bus 42, Line 40-41, Line 40-42, Line 41-42
	0.176	Bus 54, Bus 55, Bus 56, Bus 59, Line 54-55, Line 55-56, Line 55-59
	0.200	Bus 78, Bus 79, Bus 80, Line 78-79, Line 79-80, Line 80-81
	0.132	Bus 100, Bus 105, Bus 106, Bus 107, Line 100-106, Line 105-106, Line 105-107
Instantiation leaked: $\delta_{Bus77} = 0$	0.097	Bus 1, Bus 2, Bus 3, Line 1-2, Line 1-3, Line 3-5
	0.243	Bus 40, Bus 41, Bus 42, Line 40-41, Line 40-42, Line 41-42
	0.121	Bus 54, Bus 55, Bus 56, Bus 59, Line 54-55, Line 55-56, Line 55-59
	0.135	Bus 75, Bus 76, Bus 77, Bus 118, Line 75-77, Line 76-77, Line 76-118
	0.178	Bus 77, Bus 78, Bus 79, Bus 80, Line 77-78, Line 78-79, Line 79-80
	0.188	Bus 77, Bus 82, Bus 83, Bus 96, Line 77-82, Line 82-83, Line 82-96
	0.038	Bus 78, Bus 79, Bus 80, Line 78-79, Line 79-80, Line 80-81

V. CONCLUSION

In this article, the LR attack against power systems is studied in consideration of the insider threats. A security resource allocation game model is developed for the LR attack. Based on the proposed model, the information leakage by the insiders is formulated. The optimization models to calculate the best response strategies of both the system operator and attacker in the game considering the information leakage by the insider are developed. With the game model, the impacts of the information leakage by the insider in the LR attack are analyzed. It is indicated by the case studies that the defense actions of the system operator is highly important to reduce the damage of the LR attack. Meanwhile, the information leakage of the system operator's strategy on the critical measurements in the grid will provide great advantages to the attacker in the game and notably increase the expected payoff of the attacker in the LR attack, especially when the system operator is not aware of the information leakage. Further, while the composition and size of the information leakage set have considerable impacts on the payoff of the attacker, the damage of the LR attack on the grid can be increased considerably even if the information leakage probability is small. Thus, the information leakage by the insider is highly beneficial to the attacker in the LR attack on power systems. The awareness of the information leakage by the system operator is critical to obtain the optimal defense strategy and reduce the expected operation cost of the system under the LR attack. To further improve the cybersecurity of the power systems and reduce the potential damage of the LR attack, the possibility of misguiding the attacker to a sub-optimal attack strategy by the defender with the Signaling game models can be explored in future work.

REFERENCES

[1] M. S. Thomas and J. D. McDonald, *Power System SCADA and Smart Grids*. Boca Raton, FL, USA: CRC Press, 2015.

[2] M. Shahidehpour and Y. Wang, *Communication and Control in Electric Power Systems*. Piscataway, NJ, USA: IEEE Press, 2003.

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

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

[5] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE)*, College Station, TX, USA, 2017, pp. 1–8.

[6] K. Richards *et al.*, "2017 cost of cyber crime study," Ponemon Institute and Accenture, Traverse City, MI, USA, Rep., 2017.

[7] J. R. C. Nurse *et al.*, "Understanding insider threat: A framework for characterising attacks," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, 2014, pp. 214–228.

[8] K. M. Carley and G. P. Morgan, "Inadvertent leaks: Exploration via agent-based dynamic network simulation," *Comput. Math. Org. Theory*, vol. 22, no. 3, pp. 288–317, Mar. 2016.

[9] D. Liu, X. Wang, and L. J. Camp, "Mitigating inadvertent insider threats with incentives," in *Proc. 13th Int. Conf. Financial Cryptogr. Data Security (FC)*, Accra Beach, Barbados, 2009, pp. 1–16.

[10] S. Sheng, W. Yingkun, L. Yuyi, L. Yong, and J. Yu, "Cyber attack impact on power system blackout," in *Proc. IET Conf. Rel. Transm. Distrib. Netw. (RTDN)*, London, U.K., 2011, pp. 1–5.

[11] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[12] 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.

[13] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[14] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[15] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.

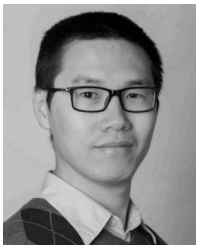
[16] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[17] Z. Li, M. Shahidehpour, A. Abdulwhab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[18] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[19] A. Abusorrah, A. Alabdulwahab, Z. Li, and M. Shahidehpour, "Minimax-regret robust defensive strategy against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2068–2079, Mar. 2019.

[20] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Elect. Power Syst. Res.*, vol. 151, pp. 12–25, Oct. 2017.
[21] H. Shayan and T. Amraee, "Network constrained unit commitment under cyber attacks driven overloads," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6449–6460, Nov. 2019.
[22] L. Lee and P. Hu, "Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks," *Int. J. Elect. Power Energy Syst.*, vol. 111, pp. 182–190, Oct. 2019.
[23] Y. Xiang, L. Wang, and N. Liu, "A framework for modeling load redistribution attacks coordinating with switching attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Chicago, IL, USA, 2017, pp. 1–5.
[24] Z. Ding, Y. Xiang, and L. Wang, "Quantifying the influence of local load redistribution attack on power supply adequacy," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Boston, MA, USA, 2016, pp. 1–5.
[25] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 889–901, Mar. 2017.
[26] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.
[27] H. Xu, A. X. Jiang, A. Sinha, Z. Rabinovich, S. Dughmi, and M. Tambe, "Security games with information leakage: Modeling and computation," in *Proc. 24th Int. Joint Conf. Artif. Intell. (IJCAI)*, Buenos Aires, Argentina, 2015, pp. 674–680.
[28] E. Litvinov, "Design and operation of the locational marginal prices-based electricity markets," *IET Gener. Transm. Distrib.*, vol. 4, no. 2, pp. 315–323, Feb. 2010.
[29] V. Sarkar and S. A. Khaparde, "DCOPF-based marginal loss pricing with enhanced power flow accuracy by using matrix loss distribution," *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1435–1445, Aug. 2009.
[30] M. M. E. A. Mahmoud, J. Mišić, K. Akkaya, and X. Shen, "Investigating public-key certificate revocation in smart grid," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 490–503, Dec. 2015.
[31] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.
[32] R. Kubo, "Detection and mitigation of false data injection attacks for secure interactive networked control systems," in *Proc. IEEE Int. Conf. Intell. Safety Robot. (ISR)*, Shenyang, China, 2018, pp. 7–12.
[33] S. Mizuno, K. Yamada, and K. Takahashi, "Authentication using multiple communication channels," in *Proc. Workshop Digit. Ident. Manag. (DIM)*, Fairfax, VA, USA, 2005, pp. 54–62.
[34] Y. Lv, T. Hu, G. Wang, and Z. Wan, "A penalty function method based on Kuhn-Tucker condition for solving linear bilevel programming," *Appl. Math. Comput.*, vol. 188, no. 1, pp. 808–813, May 2007.
[35] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in *Proc. Int. Conf. Decis. Game Theory Security (GameSec)*, London, U.K., 2015, pp. 93–112.



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

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

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

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