Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch

Journal:	*IEEE Transactions on Smart Grid*
Manuscript ID	TSG-00887-2022
Manuscript Type:	Transactions
Date Submitted by the Author:	21-Jun-2022
Complete List of Authors:	Chu, Zhongda; Imperial College London, Department of Electrical and Electronic Engineering Lakshminarayana, Subhash; University of Warwick, School of Engineering Chaudhuri, Balarko; Imperial College London, Electrical and Electronic Engineering Teng, Fei; Imperial College London, Department of Electrical and Electronic Engineering
Technical Topic Area :	Cyber-physical and cybersecurity power grid applications
Key Words:	Economic dispatch, cyber-resilience, load altering attacks

SCHOLARONE™
Manuscripts

Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch

Zhongda Chu, *Student Member, IEEE,* Subhash Lakshminarayana, *Senior Member, IEEE*
Balarko Chaudhuri, *Senior Member, IEEE* and Fei Teng, *Senior Member, IEEE*

***Abstract*—Large-scale Load-Altering Attacks (LAAs) against Internet-of-Things (IoT) enabled high-wattage electrical appliances (e.g., wifi-enabled air-conditioners, electric vehicles, etc.) pose a serious threat to power systems' security and stability. In this work, a Cyber-Resilient Economic Dispatch (CRED) framework is presented to mitigate the destabilizing effect of LAAs while minimizing the overall operational cost by dynamically optimizing the frequency droop control gains of Inverter-Based Resources (IBRs). The system frequency dynamics incorporating both LAAs and the IBR droop control are modeled. The system stability constraints are explicitly derived based on parametric sensitivities. To incorporate them into the CRED model and minimize the error of the sensitivity analysis, a recursive linearization method is further proposed. A distributionally robust approach is applied to account for the uncertainty associated with the LAA detection/parameter estimation. The overall performance of the proposed CRED model is demonstrated through simulations in a modified IEEE reliability test system.**

***Index Terms*—Economic dispatch, cyber-resilience, load altering attacks, system stability, sensitivity analysis**

I. Introduction

Internet-of-things (IoT)-enabled electrical appliances, such as WiFi-enabled air conditioners, electric vehicles, etc. are being increasingly installed, as they provide convenience to consumers. However, these devices typically do not have sophisticated security measures (such as encryption-enabled communication) incorporated in their design. Thus, they may become convenient entry points for malicious actors to gain access to the power grid. Botnet-type attacks that target a large number of these devices can severely affect power grid operations.

The topic of power grid security has gained widespread prominence in the last decade. The majority of the works focus on the security of bulk power and the associated supervisory control and data acquisition (SCADA) system [1]–[3]. In contrast, cyber attacks targeting end-user IoT-electrical appliances have only gained attention recently. Existing work on this topic can be broadly divided into two categories – (i) attack impact analysis, and (ii) detecting/localizing cyber attacks.

An unplanned and large-scale fluctuation in the system load can potentially disrupt the balance between supply and demand, subsequently leading to unsafe operating conditions. LAAs can be divided into categories depending on the type of load altered – *static* LAAs and *dynamic* LAAs. Static LAAs refer to a sudden one-time manipulation of the demand. It has been shown that such attacks lead to economic cost increment, load shedding, and/or unsafe frequency excursions [4]–[6]. Temporal fluctuations of system load and renewable energy can be exploited by the attacker to execute LAAs [7], [8]. Furthermore, low-inertia conditions caused by the growing penetration of renewable energy resources can further exacerbate the vulnerability of power grids to LAAs [8]. On the other hand, Dynamic LAA (DLAA) involves the manipulation of the demand over several time slots. In particular, it was shown that if attackers can manipulate the load in accordance with the fluctuations of system frequency, they can potentially destabilize the frequency control loop [9]. Moreover, the knowledge required to execute such attacks can be gathered from publicly-available information [10]. An analytical framework to identify buses corresponding to the least-effort destabilizing attacks was characterized in [11] using the theory of second-order dynamical systems.

Detecting and localizing LAAs is an important first step towards mitigating their destabilizing effects. Initial work in this area aimed at detecting LAAs by analyzing the power grid signals (phase angle/frequency data) in the frequency domain [12], and this method was subsequently extended to localizing the nodes that are under attack [13]. However, the framework was restricted to a linear model of power system dynamics, and cannot be extended trivially to non-linear models. An unscented Kalman filter-based approach to detect and localize LAAs was proposed in [14], which, however, does not scale well for large power grids. To overcome these limitations, reference [15] proposed the application of physics-informed machine learning techniques to detect and localize LAAs by monitoring data from phasor measurement units following the attack. The proposed framework can also estimate the attack parameters (static attack magnitude and attack controller gain for dynamic attack).

In contrast to the two streams of work, the problem of mitigating the destabilizing effects of LAAs and the corresponding impact on system operation has received limited attention, which is the main focus of this paper. Existing works on this topic mostly focus on offline security enhancements. For instance, the problem of finding the optimal locations for deploying load protection features (e.g., encryption-enabled smart devices) has been addressed in [9], [11]. Reference [16] formulates an optimization framework to obtain generator operating points to ensure that none of the transmission lines in the grid become overloaded in the event of an LAA. A data-centric edge-computing infrastructure for IoT devices in power grids is designed in [17]. Based on power grid knowledge, edge servers are equipped to enhance the security policies against IoT-based attacks. A model-free defense framework against LAAs, using machine-learning based algorithms is proposed in [18] where only static LAAs are considered. Reference [19] presents a defense policy against LAAs, which models the problem through a two-player zero-sum multistage game solved by minimax-q learning.

However, such offline mitigation measures incur significant

economic costs due to two reasons. (i) The system must be operated at an uneconomic point over the entire operating period, irrespective of whether the attack occurs or not (cyber attacks are very rare events). (ii) Since the operator has no way of having prior knowledge of the actual parameters the attackers may use, they require making *worst-case* assumptions about the attacker's capabilities (e.g., secure the power grid against all possible attack parameters).

To address these shortcomings, in this work we propose an online DLAA mitigation technique to enhance the power system's resilience to potential LAAs, named, cyber-resilient economic dispatch (CRED). The proposed method utilizes the fast and flexible control of IBR units, whose capability to enhance the system security and stability has been extensively studied and demonstrated such as in [20]–[23]. Specifically, since the DLAAs destabilize the system by decreasing the system damping, additional damping achieved through IBR droop control is supplied to the grid when an attack event is detected. It is to be noted that the scope of this study is limited to traditional electromechanical stability. The assumption is that IBRs are controlled to provide synthetic inertia and mimic the operation of SGs. Hence, the basic nature of the stability problem remains electromechanical even with large penetration of IBRs. Stability problems caused by IBRs operating in grid-following mode in conjunction with a weak network [24] in particular, are outside the scope of this study. The droop gains of the IBRs are known to influence such stability problems which would be accounted for in a future study. Additionally, the control and response of IBRs are much faster and more accurate than SGs, hence enabling the IBR units to provide the desired damping to the grid [25], [26]. Although it is possible to design or utilize more sophisticated IBR control schemes, it would significantly complicate the system dynamics and prevent it from being incorporated into optimization model, thus not being considered in this work. Moreover, the proposed approach explicitly takes the attack detection/localization results into account, including the uncertainty associated with them. It can also be easily incorporated into the conventional UC problem. Our main contributions include the following:

- We propose a CRED model to ensure the power system stability under potential LAAs. The proposed scheduling framework is implemented dynamically following LAA detection/identification to achieve stable system operation until the attack is eventually isolated in the most cost-effective manner.
- We derive the system stability constraints analytically based on parametric sensitivities. To improve the accuracy of eigenvalue sensitivities, a recursive linearization approach is proposed. The resulting constraints are further reformulated while considering the uncertainty associated with the attack parameter estimation, to fit the overall optimization model.
- The performance and effectiveness of the proposed model are demonstrated through case studies based on an IEEE Reliability Test System. The cyber-resilience improvement under different operating conditions and the corresponding cost increment as well as the impact of various factors are assessed.

The rest of the paper is organized as follows. Section II introduces the power system model considering the LAAs and the mitigation strategies. Section III derives system stability constraints, which are reformed to decrease the sensitivity error and fit the optimization model. The uncertainty of attack detection and the overall operation framework are discussed in Section IV, followed by case studies in Section V. Section VI concludes the paper.

II. System Model

In this section, the frequency dynamic model in a multi-area power system, the LAA model and the proposed mitigating strategies against the attacks are discussed.

A. Power System Modeling

We consider a power system containing a set of $\mathcal{N} = \{1, ..., N\}$ areas with the frequency and phase angle in each area assumed to be the same. Each area may include Synchronous Generators (SGs), IBRs, storage units and loads. The power system's phase angle and frequency dynamics can be described by the following set of differential equations:

$$\begin{bmatrix} I & O \\ O & \underbrace{-(M_g + M_s)}_{M} \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} 0 \\ P^L - P^C \end{bmatrix} + \begin{bmatrix} O & I \\ K^I + B & K^P + D \end{bmatrix} \begin{bmatrix} \delta \\ \omega \end{bmatrix}, \quad (1)$$

where δ, $\omega \in \mathbb{R}^N$ are vectors of phase angles and frequency deviations in each area respectively; M_g, M_s, $D \in \mathbb{R}^{N \times N}$ are diagonal matrices with their diagonal entries being the aggregated inertia of SGs, aggregated synthetic inertia from IBRs and the aggregated damping from SGs and loads; K^I, $K^P \in \mathbb{R}^{N \times N}$ are diagonal matrices with their diagonal entries being the aggregated integral and proportional gains of the governor control loop of the SGs in each area respectively; $B \in \mathbb{R}^{N \times N}$ denotes the susceptance matrix connecting different areas, and $P^L \in \mathbb{R}^N$ and $P^C \in \mathbb{R}^N$ represent the vector of aggregated demands and IBR outputs in each area.

B. Load Altering Attacks

Under LAAs, the attacker manipulates the system load by synchronously turning on or off a large amount of electrical IoT-enabled appliances. It is assumed that the demand in each area consists of two components $P^L = P^{LS} + P^{LV}$, where P^{LS} denotes the secure part of the load and P^{LV} denotes the vulnerable part of the load, which the attacker can manipulate. The system vulnerable load under LAAs is given by:

$$P^{LV} = -K^L \omega + \epsilon^L, \quad (2)$$

where $K^L \omega$ is the DLAA component that represents a time-varying load manipulation that follows the local frequency fluctuations [9] and ϵ^L is the SLAA component (one-time step-change manipulation); $K^L \in \mathbb{R}^{N \times N}$ represents the matrix of attack controller gains. It is assumed that the attacker can only monitor the frequency within the attack area, i.e., K^L

being diagonal. Combining (1) and (2) gives the power system dynamics under load altering attack:

$$\begin{bmatrix} I & O \\ O & -M \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} 0 \\ P^{LS} + \epsilon^L - P^C \end{bmatrix} + \begin{bmatrix} O & I \\ K^I + B & K^P + D - K^L \end{bmatrix} \begin{bmatrix} \delta \\ \omega \end{bmatrix}. \quad (3)$$

Using the dynamic LAA component, the attacker can alter the eigenvalues of the system indirectly by changing the elements of the matrix K^L, which is equivalent to modify the overall damping in the system. Thus, they can potentially destabilize the power system control loop [9]. Although an attack with larger K^L would lead to a less stable system, the choice of K^L is limited by the following constraint:

$$K^L_{n,n}\omega^{\max} \leq (P^{LV}_n - \epsilon^L_n)/2, \ \forall n \in \mathcal{N}, \quad (4)$$

where $K^L_{n,n}$, the n-th diagonal element is the attack gain in the n-th area and $\omega^{\max} > 0$ is the maximum permissible frequency deviation in the system. This constraint requires that the maximum value of the load to be altered by the attacker in each area should be less or equal to amount of vulnerable load after removing the static load altering attack ($P^{LV}_n - \epsilon^L_n$). The factor 2 on the RHS is due to the fact that to destabilize the system, the amount of load that needs to be compromised must allow for both over and under frequency fluctuations before the system frequency exceeds $\omega^{\max}$.

C. Mitigating Actions Against LAAs

The attackers have the capability to destabilize the system if the amount of the vulnerable load is large enough. Therefore, it is necessary for the system operators to maintain the system stability with proper measures given the potential LAAs. The mitigation strategies considered here is the frequency droop control implemented in the IBRs, due to their fast and accurate active power control. Furthermore, the droop structure is relatively simple and can be incorporated into the system scheduling process, enabling dynamic optimization and implementation immediately after the LAA detection. Moreover, the droop control is equivalent to providing system damping which is exactly what the attacker manipulates through the DLAA, thus being effective in counteracting the attack and stabilizing the system. Note that the droop control has been proposed and studied mainly for the purpose of frequency support after system disturbances. However, in this work the frequency droop control from IBRs is controlled to supply additional system damping during the attack period such that the overall system stability can be ensured.

The output power from IBRs, P^C can then be expressed as

$$P^C = P^{C*} - K^C\omega, \quad (5)$$

where P^{C*} is the total power reference of IBRs in each area and $K^C\omega$ represent the power deviation according to the local frequency. $K^C \in \mathbb{R}^{N\times N}$ is a diagonal matrix with the entries being the aggregated droop gains in each area. Combining (1), (2) and (5) gives the power system dynamics with LAAs and the droop response from IBRs.

$$\underbrace{\begin{bmatrix} I & O \\ O & -M \end{bmatrix}}_{-\mathcal{A}} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} 0 \\ P^{LS} + \epsilon^L - P^{C*} \end{bmatrix} + \underbrace{\begin{bmatrix} O & I \\ K^I + B & K^P + D - K^L + K^C \end{bmatrix}}_{\mathcal{B}} \begin{bmatrix} \delta \\ \omega \end{bmatrix}. \quad (6)$$

It is evident that with appropriate selection of the droop control gains from IBRs given the estimation or prediction of the potential attacks [15], the system stability can be maintained. Remarkably, the droop response of IBRS are considered as decision variables due to their fast control whereas the proportional control gains (K^P) of synchronous generators are considered to be fixed.

III. System Stability Constraint Derivation and Reformulation

In this section, the system stability constraints under LAAs are derived based on system eigenvalues and sensitivity analysis. To ensure an accurate approximation, a recursive linearization approach is further proposed. The resulting conditional constraints are effectively reformulated to fit the overall optimization structure while considering the uncertainty associated with the attack gain estimation.

A. System Stability Constraints

Denote the eigenvalues of system (6) by $\lambda_i \in \mathbb{C}$ and the associated right and left eigenvector by $\mathbf{z}_j$, $\mathbf{y}_j \in \mathbb{C}^{2N}$. The system becomes unstable if there exists at least one eigenvalue λ_i, such that $\Re(\lambda_i) > 0$. Here, only stability constraint is considered but if the requirement is for the oscillations to settle within a stipulated time, the constraint boundary can be shifted to the left of the imaginary axis to ensure a minimum settling time. Therefore, to ensure the system stability, the following constraint must hold:

$$\Re(\hat{\lambda}_i) = \Re(\lambda^0_i) + \sum_{n\in\mathcal{N}} \Re\left(\frac{\partial\lambda^0_i}{\partial K^L_{n,n}}\right) K^L_{n,n} + \sum_{n\in\mathcal{N}} \Re(\frac{\partial\lambda^0_i}{\partial K^C_{n,n}}) K^C_{n,n} < 0, \ \forall i = 1, ..., 2N, \quad (7)$$

where $\hat{\lambda}_i$ is the estimated i-th eigenvalue using sensitivities and λ^0_i is the eigenvalue of the system without the LAAs and the additional droop control from IBRs. The relationship $\Re(\lambda^0_i) < 0, \forall i = 1, ..., 2N$ must hold since the system is stable without attacks. $\frac{\partial\lambda^0_i}{\partial K^L_{n,n}} / \frac{\partial\lambda^0_i}{\partial K^C_{n,n}}$ are the eigenvalue sensitivities with respect to the n-th diagonal element in K^L/K^C matrix. The analytical expressions for the sensitivity factors can be derived using the theory of second-order dynamical system [11]:

$$\frac{\partial\lambda^0_i}{\partial K^L_{n,n}} = -\frac{\partial\lambda^0_i}{\partial K^C_{n,n}} = -\mathbf{y}_i^\intercal \left[\lambda^0_i \frac{\partial\mathcal{A}}{\partial K^L_{n,n}} + \frac{\partial\mathcal{B}}{\partial K^L_{n,n}}\right] \mathbf{z}_i, \quad (8)$$

where,

$$\frac{\partial \mathcal{A}}{\partial K^L_{n,n}} = O \tag{9a}$$

$$\frac{\partial \mathcal{B}}{\partial K^L_{n,n}} = \begin{bmatrix} O & O \\ O & -I_{n,n} \end{bmatrix}. \tag{9b}$$

We define $I_{n,n}$ as a matrix whose $(n,n)^{\text{th}}$ element is one if there is a DLAA in the n-th area, and all the others are zero.

Moreover, the limits of $K^L_{n,n}$ and $K^C_{n,n}$ in an actual system have to be considered. The former is discussed in (4), whereas for $K^C_{n,n}$, the following constraint applies:

$$P^{C*}_n + K^C_{n,n}\omega^{\max} \le P^{C,\max}_n \tag{10a}$$

$$P^{C*}_n - K^C_{n,n}\omega^{\max} \ge 0, \tag{10b}$$

where $P^{C,\max}_n$ is the aggregated maximum available active power from IBRs according to the MPPT control in the n-th area. Constraint (10) ensures adequate deloaded active power and sufficiently large power output during normal operation (without LAAs) to provide desired droop response following the frequency oscillation on both sides triggered by the attack. It is clear that a larger $K^C_{n,n}$ leads to a more stable system but inevitably more operation cost. This trade-off will be balanced in the proposed cyber-resilient economic dispatch model.

B. Recursive Linearization Approach

Since the system stability constraint in (7) is derived based on the sensitivity analysis, it provides a satisfying approximation only if the $K^L_{n,n}$ and $K^C_{n,n}$ are relatively small. However, this may not always be the cases in reality. To illustrate this issue, first rewritten (7) giving the relationship in (8):

$$\Re(\lambda^0_i) + \sum_{n\in\mathcal{N}} \Re\left(\frac{\partial \lambda^0_i}{\partial K^L_{n,n}}\right) \underbrace{(K^L_{n,n} - K^C_{n,n})}_{K^{L-C}_{n,n}} < 0, \quad \forall i = 1, ..., 2N. \tag{11}$$

An example demonstrating the linearization performance based on (11) is shown in Fig. 1 with only one eigenvalue plotted for simplicity. It is observed that as $K^{L-C}_{n,n}$ decreases from zero, the real part of the eigenvalue increases, which results in an unstable system if it becomes positive. However, the error between the true values and the approximations based on (11) gradually increases in this process due to the larger distance to the linearization point ($K^{L-C}_{n,n} = 0$). In addition, since the system stability depends on the sign of the eigenvalues, good approximations should always be ensured for all $K^{L-C}_{n,n}$ that renders eigenvalues with negative and slightly positive real parts, e.g., $[-3.5, 0]$ in this case. Therefore, the approximations in Fig. 1 give unsatisfying results because of the errors around zero. Although this may not occur for certain system parameters, there is no systematic guarantee based on the formulation in (11).

In order to address this problem, a piecewise decision-dependent recursive linearization approach is proposed with the detailed steps shown in Algorithm 1. After the initialization, the sensitivity range $\phi_{i,n}$, within which an accurate approximation is desired, is determined first. For instance, $\phi_{i,n} = [-3.5, 0]$ in the case of Fig. 1. Gradually vary the

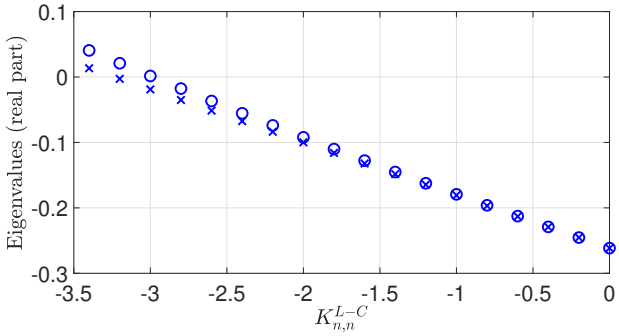

Fig. 1: Real part of system eigenvalue under single-point LAAs. Circles: true values, Crosses: estimated values.

Algorithm 1 Recursive Linearization Algorithm

1: Set $m = 0$, $l = 0$, $\varepsilon^m = 0$, $\Delta\phi^{(l)}_{i,n} = 0$ and $\mathcal{M}_{i,n} = \{m\}$
2: Determine the sensitivity range, $\phi_{i,n} = [\underline{\phi}_{i,n}, 0]$
3: **while** $\Delta\phi^{(l)}_{i,n} \ge \underline{\phi}_{i,n}$ **do**
4: Obtain the new linearization point, $\Delta\phi^m_{i,n} = \Delta\phi^{(l)}_{i,n}$
5: Calculate the eigenvalue at this point, $\lambda^m_{i,n} = \lambda_i|_{K^{L-C}_{n,n}=\Delta\phi^m_{i,n}}$
6: Calculate the sensitivity at this point, $\frac{\partial\lambda^m_{i,n}}{\partial K^L_{n,n}}$
7: **while** $\varepsilon^m \le \varepsilon^{\lim}$ **do**
8: $l = l + 1$
9: Move along the sensitivity range, $\Delta\phi^{(l)}_{i,n} = \Delta\phi^{(l-1)}_{i,n} - \varepsilon_\phi$
10: Calculate the true eigenvalue, $\lambda^{(l)}_{i,n}$
11: Calculate the estimated eigenvalue, $\hat{\lambda}^{m,(l)}_{i,n}$
12: Compute the approximation error, $\varepsilon^m = \left|\Re(\lambda^{(l)}_{i,n}) - \Re(\hat{\lambda}^{m,(l)}_{i,n})\right|$
13: **end while**
14: $\mathcal{M}_{i,n} = \mathcal{M}_{i,n} \cup \{m\}$
15: $m = m + 1$
16: Reset the approximation error, $\varepsilon^m = 0$
17: **end while**
18: Return $\mathcal{M}_{i,n}$, $\boldsymbol{\varphi}_{i,n}$ and $\boldsymbol{\partial\varphi}_{i,n}$

auxiliary $\Delta\phi^{(l)}_{i,n}$ from 0 to $\underline{\phi}_{i,n}$ with a pre-defined fixed step, ε_ϕ. At each step, calculate the true eigenvalue, $\lambda^{(l)}_{i,n}$, by setting $K^{L-C}_{n,n} = \Delta\phi^{(l)}_{i,n}$ and the estimated eigenvalue, $\hat{\lambda}^{m,(l)}_{i,n}$, based on the sensitivity evaluated at the latest linearization point $K^{L-C}_{n,n} = \Delta\phi^m_{i,n}$, which are defined as follows:

$$\lambda^{(l)}_{i,n} = \lambda_i|_{K^{L-C}_{n,n}=\Delta\phi^{(l)}_{i,n}} \tag{12a}$$

$$\hat{\lambda}^{m,(l)}_{i,n} = \lambda^m_{i,n} + \frac{\partial\lambda^m_{i,n}}{\partial K^L_{n,n}}(\Delta\phi^{(l)}_{i,n} - \Delta\phi^m_{i,n}), \tag{12b}$$

where $\lambda^m_{i,n}$ is the i-th eigenvalue of the system with potential attack or IBR droop control in area n, evaluated at the m-th linearization point (Step 5), and $\frac{\partial\lambda^m_{i,n}}{\partial K^L_{n,n}}$ is the associated sensitivity based on (8).

As long as the approximation error is smaller than a pre-specified limit $\varepsilon^{\lim}$, the current linearization point and the associated sensitivity are acceptable. However, once the error

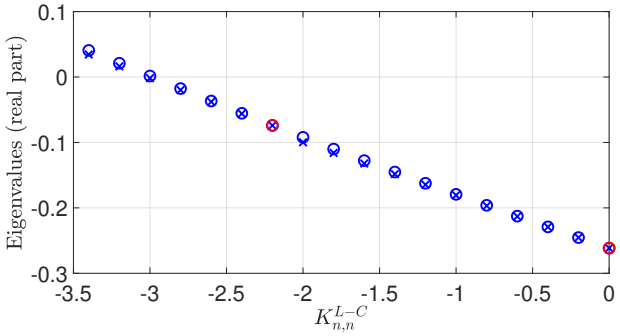

Fig. 2: Real part of system eigenvalue using proposed algorithm. Circles: true values, Crosses: estimated values.

becomes larger than the limit, reset the approximation error. Then, choose a new linearization point by setting $\Delta\phi^m_{i,n} = \Delta\phi^{(l)}_{i,n}$ and calculate the eigenvalue and the sensitivity at this point. This process is repeated until all the values in the sensitivity range are evaluated (in a discrete manner). To formulate the system stability constraints, all the linearization points and the associated sensitivities are collected:

$$\boldsymbol{\varphi}_{i,n} = \left\{ \phi^m_{i,n} \middle| \, \forall\, m \in \mathcal{M}_{i,n} \right\} \tag{13a}$$

$$\boldsymbol{\partial\varphi}_{i,n} = \left\{ \frac{\partial \lambda^m_{i,n}}{\partial K^L_{n,n}} \middle| \, \forall\, m \in \mathcal{M}_{i,n} \right\}. \tag{13b}$$

Note that theoretically this algorithm applies for all $i = 1, ..., 2N$ and $n \in \mathcal{N}$. However, in practice, not all the eigenvalues and their sensitivities with respect to all the areas are needed. Given the system information and the prediction of the potential attacks, it is very likely that the numbers of vulnerable eigenvalues and sensitives are limited. Those eigenvalues that are barely influenced by the attack and the IBR droop control, thus never entering the right-half plane, can be neglected.

An example of the linearization performance applying Algorithm 1 is depicted in Fig. 2 where the red circles represent the linearization point, i.e., $\phi^m_{i,n} \in \{0, -2.2\}$ in this case. It is observed that the gradually increasing approximation error due to the deviation from the linearization point is reset at $K^{L-C}_{n,n} = -2.2$, where a new linearization point is defined. Therefore, with the proposed recursive linearization approach, any desired accuracy, specified by ε^{lim}, can be achieved within the entire sensitivity range.

C. System Stability Constraint Reformulation

The system stability constraint (7) which is derived based on sensitivities evaluated at one single linearization point needs to be adapted considering Algorithm 1:

$$\Re\left(\lambda^0_i + \sum_{n\in\mathcal{N}} \mathcal{F}_n\left(K^{L-C}_{n,n}\right)\right) < 0,\ \forall i = 1, ..., 2N, \tag{14}$$

where $\mathcal{F}_n(\cdot)$ is the eigenvalue variation due to the attack or IBR droop control in the n-th area. It is defined as follows:

$$\mathcal{F}_n = \begin{cases} \frac{\partial \lambda^0_i}{\partial K^L_{n,n}} K^{L-C}_{n,n}, & \text{if } K^{L-C}_{n,n} \in (\phi^1_{i,n}, \phi^0_{i,n}] \\ \ldots & \\ \frac{\partial \lambda^m_i}{\partial K^L_{n,n}}(K^{L-C}_{n,n} - \phi^m_{i,n}) & \\ \quad +(\lambda^m_i - \lambda^0_i), & \text{if } K^{L-C}_{n,n} \in (\phi^{m+1}_{i,n}, \phi^m_{i,n}] \\ \ldots & \\ \frac{\partial \lambda_i^{|\mathcal{M}_{i,n}|-1}}{\partial K^L_{n,n}}(K^{L-C}_{n,n} - \phi^{|\mathcal{M}_{i,n}|-1}_{i,n}) & \\ \quad +(\lambda_i^{|\mathcal{M}_{i,n}|-1} - \lambda^0_i), & \text{if } K^{L-C}_{n,n} \in [\underline{\phi}_{i,n}, \phi^{|\mathcal{M}_{i,n}|-1}_{i,n}] \end{cases}. \tag{15}$$

Depending on the range of $K^{L-C}_{n,n}$, the sensitivity of the nearest linearization point on its right is used. However, since $K^{L-C}_{n,n}$ is essentially a decision variable, (14) is a decision-dependent constraint, which cannot be incorporated into the optimization problem directly. To address this problem, $|\mathcal{M}_{i,n}|$ binary variables, $\left\{ z^m_{i,n} \middle| \, m \in \mathcal{M}_{i,n} \right\}$, are introduced for each i and n to indicate to which interval $K^{L-C}_{n,n}$ belongs:

$$z^m_{i,n} = \begin{cases} 1 & \text{if } \phi^{m+1}_{i,n} < K^{L-C}_{n,n} \le \phi^m_{i,n} \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

Equation (16) can be rewrite in the following form by defining ancillary binary variables $z^{m1}_{i,n}$, $z^{m2}_{i,n}$, $\forall m \in \mathcal{M}_{i,n}$:

$$z^{m1}_{i,n} = \begin{cases} 1 & \text{if } \phi^{m+1}_{i,n} < K^{L-C}_{n,n} \\ 0 & \text{otherwise} \end{cases} \tag{17a}$$

$$z^{m2}_{i,n} = \begin{cases} 1 & \text{if } K^{L-C}_{n,n} \le \phi^m_{i,n} \\ 0 & \text{otherwise} \end{cases} \tag{17b}$$

$$z^m_{i,n} = z^{m1}_{i,n} + z^{m2}_{i,n} - 1. \tag{17c}$$

As a result, the conditional constraints (17) can be transformed into linear constraints, $\forall n \in \mathcal{N}$:

$$0 \le \phi^{m+1}_{i,n} - K^{L-C}_{n,n} + \mathbf{M} z^{m1}_{i,n} < \mathbf{M} \tag{18a}$$

$$0 < K^{L-C}_{n,n} - \phi^m_{i,n} + \mathbf{M} z^{m2}_{i,n} \le \mathbf{M} \tag{18b}$$

$$z^m_{i,n} = z^{m1}_{i,n} + z^{m2}_{i,n} - 1 \tag{18c}$$

$$z^m_{i,n},\ z^{m1}_{i,n},\ z^{m2}_{i,n} \in \{0, 1\} \tag{18d}$$

where $\mathbf{M} > 0$ is a sufficiently large constant. With the binary variables $z^m_{i,n}$, the conditional constraints (15) can be converted to:

$$\mathbf{F}_n = \sum_{m\in\mathcal{M}_{i,n}} \mathbf{F}^m_n z^m_{i,n}, \tag{19}$$

where

$$\mathbf{F}^m_n = \frac{\partial \lambda^m_i}{\partial K^L_{n,n}}(K^{L-C}_{n,n} - \phi^m_{i,n}) + (\lambda^m_i - \lambda^0_i),\ \forall m \in \mathcal{M}_{i,n}. \tag{20}$$

The only nonlinearity in (19), (20) is the term $K^{L-C}_{n,n} z^m_{i,n}$, which is the product of a continuous and a binary variable. This can be easily linearized through the standard Big-M method, which is not covered here. Finally, the system stability constraint under LAAs and the IBR droop control can be

obtained by combining (14) with $\mathcal{F}_n$ being replaced by $\mathbf{F}_n$ together with (18), (19) and (20):

$$\Re\Bigg(\lambda_i^0+\sum_n\Bigg(\sum_m\Big(\frac{\partial\lambda_i^m}{\partial K_{n,n}^L}(K_{n,n}^{L-C}-\phi_{i,n}^m) + (\lambda_i^m-\lambda_i^0)\Big)z_{i,n}^m\Bigg)\Bigg)<0,\ \forall i=1,...,2N. \quad (21)$$

IV. Incorporating Uncertainty of Attack Detection Into CRED And Overall System Operation

The framework presented thus far assumes perfect knowledge of the attack parameters K^L. In real-world operation, attack mitigation operation such as CRED follows the attack detection/attack parameter estimation phase. Existing works [13], [15] adopt a data-driven approach for this purpose using frequency/phase angle data monitored by phasor measurement units. However, due to the stochastic nature of the detection algorithms (e.g., machine learning based detectors proposed in [15]), and factors such as sensor measurement noise, the predicted attack parameters incur estimation errors. In this section, we present a framework to incorporate such errors into the CRED algorithm and provide details on how CRED can be incorporated into the overall system operation.

A. Distributionally Robust Chance Constraint

In order to account for the uncertainty associated with the estimation of LAAs parameters, the system stability constraints are further reformulated into distributionally robust form. Assume that the first and second moment of LAAs gains are known whereas the detailed distribution is unknown. For instance, the aforementioned first and second moments can be computed numerically by analyzing data traces obtained from the attack detection/parameter estimation process (more details are provided in the Section V).

Therefore, the random variable $K_{n,n}^L, \forall n \in \mathcal{N}$ can be modeled by the following ambiguity set:

$$\mathcal{P}=\Big\{\mathbf{D}\in\Phi(K_{n,n}^L):\mathrm{E}^{\mathbf{D}}(K_{n,n}^L)=\bar{K}_{n,n}^L,\ \mathrm{Var}^{\mathbf{D}}(K_{n,n}^L)=\sigma_n^2\Big\}, \quad (22)$$

where $\Phi(K_{n,n}^L)$ denotes the set of all probability distributions on $K_{n,n}^L$; $\bar{K}_{n,n}^L$ and σ_n^2 denote the mean and variation of $K_{n,n}^L$. In addition, assume that the attacks in different areas are independent with each other, i.e.,

$$\mathrm{cov}\left(K_{n,n}^L,K_{m,m}^L\right)=0,\ \ \forall n,m\in\mathcal{N},n\neq m. \quad (23)$$

By modifying (21), the distributionally robust chance constraint of system stability, $\forall i=1,...,2N$, can be thus written as:

$$\inf_{\mathbf{D}\in\mathcal{P}}\Pr\Bigg\{\Re\Bigg(\lambda_i^0+\sum_n\Bigg(\sum_m\Big(\frac{\partial\lambda_i^m}{\partial K_{n,n}^L}(K_{n,n}^L-K_{n,n}^C-\phi_{i,n}^m) + (\lambda_i^m-\lambda_i^0)\Big)z_{i,n}^m\Bigg)\Bigg)<0\Bigg\}\geq\eta, \quad (24)$$

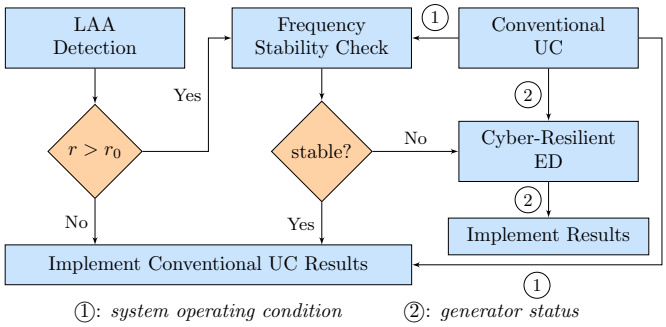

Fig. 3: General framework of the proposed model in system operation.

where $\eta\in(0,1)$ is the confidence level specified by system operators. According to *Theory 3.1* in [27], the above distributionally robust chance constraint is equivalent to:

$$\Re\Bigg(\lambda_i^0+\sum_n\Bigg(\sum_m\Big(\frac{\partial\lambda_i^m}{\partial K_{n,n}^L}(\bar{K}_{n,n}^L+k_\eta\sigma_n - K_{n,n}^C-\phi_{i,n}^m)+(\lambda_i^m-\lambda_i^0)\Big)z_{i,n}^m\Bigg)\Bigg)<0 \quad (25a)$$

$$k_\eta=\sqrt{\frac{\eta}{1-\eta}}, \quad (25b)$$

which ensures system stability given certain confidence level.

B. Overall System Operation Framework

The overall framework of the proposed CRED is integrated in the system scheduling model as illustrated in Fig. 3. Since the LAAs are low frequency high impact events, it is economically inefficient to run the CRED algorithm during normal system operation. Instead, at this stage, conventional Unit Commitment (UC) with N-1 frequency security constraints (maximum RoCoF, frequency nadir and steady-state frequency) as proposed in [28], is conducted and the LAA detection is constantly performed. The objective of the conventional UC problem is to minimize the expected cost over all nodes in the given scenario tree:

$$\min\sum_{n\in\mathcal{N}}\pi(n)\left(\sum_{g\in\mathcal{G}}C_g(n)+\Delta t(n)c^sP^s(n)\right) \quad (26)$$

where $\pi(n)$ is the probability of scenario $n\in\mathcal{N}$ and $C_g(n)$ is the operation cost of unit $g\in\mathcal{G}$ in scenario n including startup, no-load and marginal cost; $\Delta t(n)c^sP^s(n)$ represents the cost of the load shedding in scenario n with the three terms being the time step of scenario n, load shedding cost and shed load. The objective function (26) is subjected to a number of constraints. Due to the space limitation, all the conventional UC constraints such as those related to thermal generation units, power balance and frequency security are not listed in the paper. The readers can refer [28], [29] for more details regarding the constraints and scenario tree building. Note that at this stage, the system stability constraints are not included in the scheduling model.

However, if a potential LAA is detected, indicated by a pre-defined criterion, $r > r_0$, (e.g., using existing approaches [15]), then the system resilience needs to be guaranteed under this circumstance. The operating conditions obtained from conventional UC are checked first, against system stability given the estimation of LAA. Since the system parameters, operating conditions and the attack information are known, this process can be conducted fast and easily by assessing the eigenvalues of the system (25), thus not being covered here. A stable system renders no further action and the results from conventional UC are implemented, whereas an unstable system requires CRED algorithm to be implemented in order to ensure stable system operation (until the attack can be potentially isolated) and avoid potential blackouts.

The CRED takes the input of generator status from conventional UC and outputs the resilient system operating conditions. The optimization model of the CRED remains the same as the conventional UC, except that the generator states are fixed according to the conventional UC and the constraint (25) is added to guarantee the system stability under the detected LAAs. Constraint (25) requires IBR droop control and deloading of RES, which influences generation cost and the optimization objective as defined in (26). Larger droop gains lead to a more stable system with higher operational cost. This trade-off can be balanced within the proposed CRED framework, ensuring the system stability under LAAs in a most cost-effective manner. Note that if the actual attack parameters (such as attack controller gain K^L) cannot be identified accurately, then the system operator can always use the worst-case attack parameters in the implementation of CRED framework, by replacing (25) with (21). Additionally, during the CRED process, we assume that the loss of generation and the LAAs would not occur simultaneously.

V. Case Studies

In this section, the effectiveness of the proposed CRED algorithm and its impact on system operation are assessed through simulations in the modified IEEE Reliability Test System (72 buses, 33 machines). The system is divided into three areas and the parameters are available in [30], [31]. In addition, wind generation is added in Area 2 to realize different IBR penetrations and it is assumed that the attack only occurs in Area 2 since an attack in other areas has little impact on system operation as demonstrated in Section V-C. Other system parameters are set as follows: load demand $P^D \in [4.79, 8.55]$ GW, load damping $D = 0.5\% P^D/1$ Hz, base power $P_B = 1$GW, confidence level $\eta = 95\%$. The frequency limits of nadir, steady-state value and RoCoF are set as: 0.8 Hz, 0.5 Hz and 0.5 Hz/s respectively. The weather conditions are obtained from online numerical weather prediction [32]. We consider an optimization problem with a time horizon of 24 hours and time step of 1 hour, which is solved by Gurobi (8.1.0) on a PC with Intel(R) Core(TM) i7-7820X CPU @ 3.60GHz and RAM of 64 GB. Note that the SI from IBRs are not considered, i.e., $M_s = 0$ in (1), for all the case studies except in Section V-D where its impact is explicitly investigated.

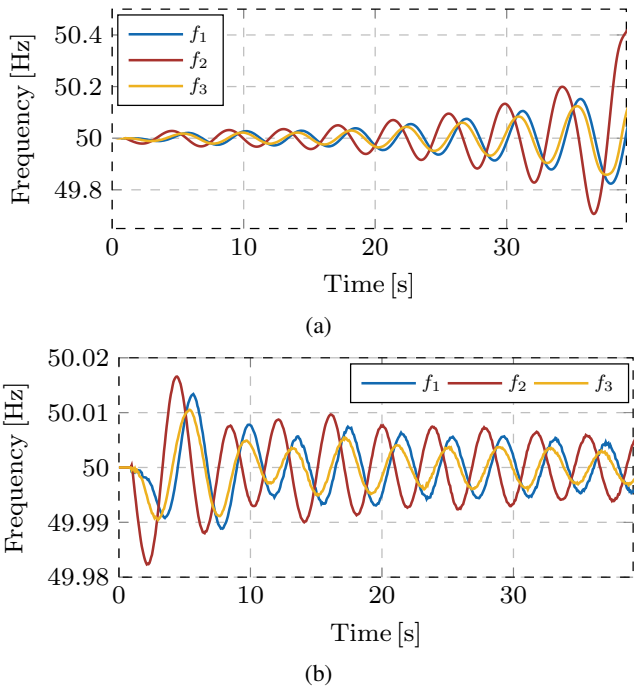

Fig. 4: System frequency evolution after a small step disturbance at $t = 1$ s: (a) without CRED; (b) with CRED.

A. Time domain simulation

The effectiveness of the proposed CRED in terms of maintaining system stability is validated through time domain simulation. Fig. 4 depicts the frequency dynamics of the studied system under LAA at Area 2 with and without the CRED, where $f_{i\in\{1,2,3\}}$ represents the averaged frequency of the i-th area. The same amount of accessible vulnerable load (30%) to the attacker is assumed for both situations. In order to assess the system stability, the frequency variations are triggered by applying a small step disturbance at $t = 1$ s. In Fig. 4a, the system becomes unstable under LAAs without CRED, where the frequencies in all the areas oscillate with increasing magnitude. f_2 is spotted with the largest oscillation magnitude as the LAA is applied in this area. This growing frequency deviation would eventually lead to generator trips and even cascade failures, endangering the system operation. On the contrary, with the proposed CRED (Fig. 4b), the LAA with the same magnitude cannot destabilize the system, since there is enough damping in the system and the oscillations due to the LAA gradually attenuate. Note the difference in the frequency range of the two sub-figures.

Other parameters related to the two systems in Fig. 4 are listed in Table I, where K^L and K^C are the DLAA and IBR droop gains; P_{res}, P^W, P^G and Cost represent the reserved wind power for IBR droop response, total power from

TABLE I: System Parameters w/o and with CRED

CRED	K^L [p.u.]	K^C [p.u.]	P_{res} [GW]	P^W [GW]	P^G [GW]	Cost [k£]
w/o	26.70	0	0	3.82	4.74	68.73
with	26.70	18.85	0.30	3.51	5.04	80.21

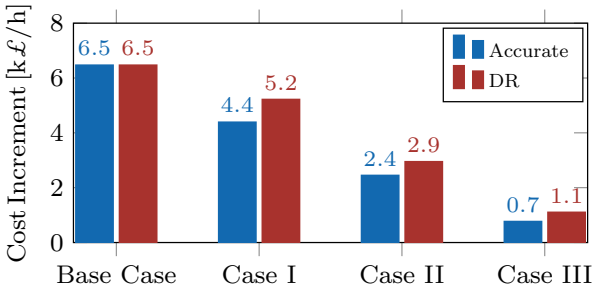

Fig. 5: Cost increment of CRED under different attack knowledge.

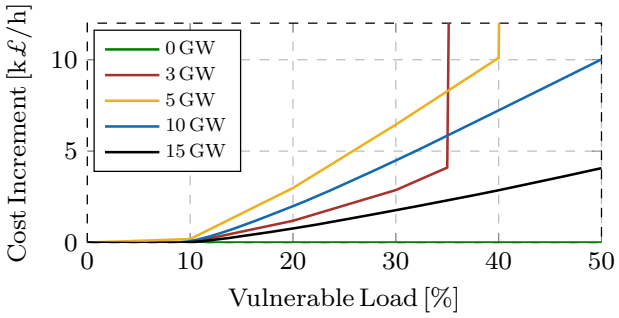

Fig. 6: Impact of wind penetration and vulnerable load on system operation cost considering potential LAAs.

wind and synchronous generation and system operation cost respectively. It is observed that to maintain system stability 0.6 GW of wind power is deloaded, hence more power from SGs and larger operation cost.

B. Assessment of CRED with various knowledge of attack parameters

The additional system operation cost to ensure the cyber-resilience is shown in Fig. 5. Three different situations are considered: (1) worst case assumption of the attack parameter where the system operator has no estimation of the actual attacks and assumes the attacker has access to all the vulnerable load in the system (Base Case); (2) accurate estimation of the actual attacks where the real attack gains can be predicted perfectly (blue bars in Case I-III); (3) Distributional Robust (DR) case where only the first and second moments of the attack parameters are assumed to be known based on some attack estimation methods (red bars in Case I-III). In particular, for (3), we implement the sparse identification of non-linear dynamics (SINDy) algorithm proposed in [15] for LAAs attack parameter estimation (we choose the SINDy algorithm as the algorithm is robust and performs well over a wide range of system parameters) over 1000 runs, and compute the required first and second moments numerically as shown in Table II. Note that the installed wind capacity in Area 2 for all the cases is 5 GW and the total vulnerable load is 30% of the load in this area. Since attacks with the same magnitude at different hours of a day may have different effect on system operation, the cost increment in this work is the averaged value among the cost increment due to the attack at each hour of the day.

It can be observed from the figure that Base Case leads to largest cost increment since it assumes all the vulnerable load can be accessed by the attacker to generate the attack, thus being most conservative. In this case, the accurate and DR approaches make no difference. Furthermore, Case I to Case III represent the circumstances where the attacker has 80%, 60% and 40% accessibility to the entire vulnerable load respectively. As expected, when the attacker has lower accessibility to the vulnerable load, less additional cost is generated for both accurate estimation and DR approach, to maintain the system stability. In all these cases, the DR approach causes slightly larger cost increment compared with accurate estimation due to the uncertainty management associated with the attack parameter estimation. However, it is also clear that the proposed DR approach can reduce the attack-induced operation cost giving actual estimation of the attack parameters compared with the worst case assumption.

Note that the dynamic simulation shown in Fig. 4b corresponds to the accurate attack estimation case. Since the DR case presents a very similar trend except a slightly faster attenuation rate due to the larger damping, it is not included.

TABLE II: Attack Parameters Associated with Fig. 5

	Base Case	Case I	Case II	Case III
K^L [p.u.]	22.31	16.96	13.50	9.11
$\tilde{K}^L$ [p.u.]	22.31	17.59	13.19	8.80
σ [p.u.]	0	0.48	0.36	0.24

C. Impact of wind penetration on LAAs and CRED

In conventional power system where the main power sources are SGs, the LAAs may not be able to destabilize the system as there is sufficient damping in the system. However, the consequence of LAAs could become more obvious with higher wind penetration where less damping from SGs is available. To demonstrate this effect, Fig. 6 depicts system cost increment due to the attack with increasing percentage of vulnerable load, where each line represents a different installed wind capacity.

If no wind generation is installed in the system (green line), the LAAs do not influence the system operation cost because the SGs are capable of maintaining the system stability even if 50% of the load in Area 2 is vulnerable. Furthermore, as the installed wind capacity increases to 3 GW and 5 GW, less SGs are dispatched in the system, making the system less stable. Therefore, additional damping (K^C) is required from IBRs to maintain system stability under the LAAs, which results in the deloading of wind power and more dispatched power from SGs, hence more operation cost. A larger wind penetration and higher vulnerable load make the above effect more evident, corresponding to higher cost increment. Notably, after the vulnerable load increases to about 35% and 40% in the cases of 3 GW and 5 GW respectively, the system operation cost grows dramatically. This is because there is not enough wind power to be deloaded for more damping provision and some of the load has to be curtailed to maintain system stability, thus generating significant load shedding cost.

However, as the wind penetration continues increasing (blue and black curves), we notice that the cost increment due to the attack starts to decrease, since to ensure the N-1 frequency security constraints, certain amount of SGs has

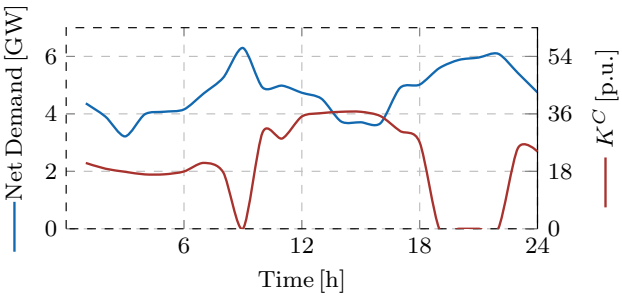

Fig. 7: Relationship between net demand and K^C.

to remain connected in the system and more wind power is available to supply additional damping, making it easier to maintain system stability. Moreover, the substantial cost increase induced by the load shedding disappears with the sufficient wind power.

An example of the additional damping from IBRs (K^C) under the attack at different hours in the day, and its relationship with the net demand ($P^D - P^W$) in the system are depicted in Fig. 7, where the vulnerable load is 30% of the total load and the wind capacity is 5 GW. A clear negative correlated relationship can be spotted, i.e., higher net demand leads to less K^C from wind generation. This is due to the reason that more SGs are dispatched online to supply the higher net demand, hence less damping from IBRs are needed to maintain system stability. Note that the equivalent damping from SGs is around 20 p.u. based on their own capacities [30].

D. Impact of synthetic inertia provision on CRED

During the conventional UC process in Fig. 3, the N-1 frequency security constraints are considered such that the constraints of frequency metrics will not be violated. The previous section (Sec. V-C) only utilizes the inertia and primary frequency responses from SGs to ensure the frequency security. Alternatively, fast frequency responses from IBRs can also help to maintain the frequency constraints. Specifically, we consider the Synthetic Inertia (SI) provision from wind turbines [28] and its influences on the LAAs and the CRED are analyzed here. Notably, since SI is provided using the stored kinetic energy of wind turbines, there is no additional cost due to SI provision.

The results are illustrated in Fig. 8, where cost increments with various wind penetration are considered. The solid and

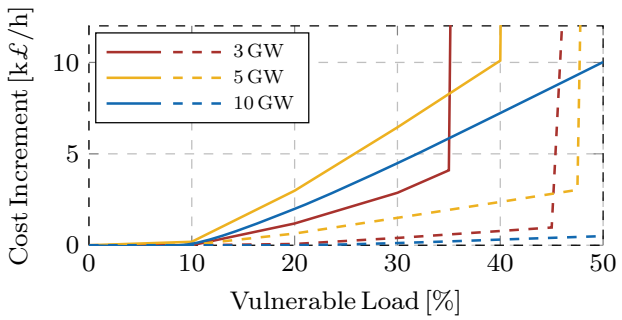

Fig. 8: Impact of synthetic inertia provision on CRED. Solid lines: without SI, Dashed lines: with SI.

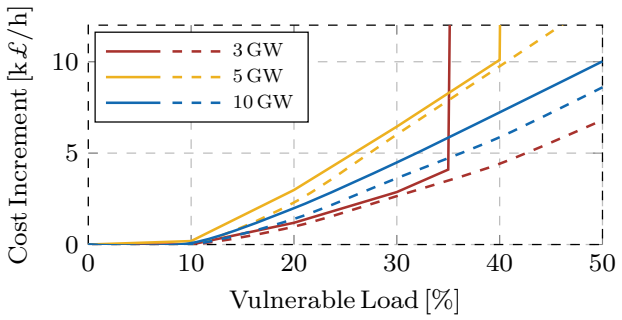

Fig. 9: Impact of energy storage on CRED. Solid lines: without storage, Dashed lines: with storage.

dashed lines represent the situation without and with SI provision respectively. Compared with the previous situation (without SI), once SI is incorporated into the convention UC process, the additional operation cost to ensure the system resilience under LAAs reduces significantly at different wind penetrations. This is due to the fact that the synthetic inertia from the wind turbines in Area 2 decreases the eigenvalue sensitivities with respect to the attacks, making the system more stable. Therefore, attacks with the same magnitude as in the no SI cases have less effects on destabilizing the system, thus less cost increment. For the same reason, the percentage of vulnerable load after which load shedding is needed to ensure system stability in the cases with 3 GW and 5 GW wind power also increases by about 10% and 8% respectively.

E. CRED under different battery energy storage conditions

In power systems with high wind penetration, it is often the situation that certain amount of battery energy storage is preferred to better utilize the renewable energy and mitigate the uncertainty in the system. This subsection investigates how the battery energy storage would influence the resilience of the system under LAAs. Fig. 9 presents the system operation cost increment to maintain system stability under LAAs without (solid curves) and with (dashed curves) battery energy storage. The parameters of battery energy storage are shown in Table III, with $\mathrm{SoC}_{\min}$, $\mathrm{SoC}_{\max}$, η_b, $|\bar{P}_b|$ and E_b denote the minimum, maximum state of charge, efficiency, maximum (dis)charging power and energy capacity. It is observed that the overall impact of battery energy storage on the system operation against the LAAs is not very remarkable for most of the cases in Fig. 9, where there is no load shedding. This is because the energy usages with battery storage in the system has already been optimized in the conventional UC problem and once the attack is detected, the additional cost due to the power re-dispatch would not change considerably compared with the case where no storage is installed in the system. Hence, the dashed lines are slightly below the solid lines with the same color. However, the load shedding in the cases of 3 GW and 5 GW wind capacity disappears after including

TABLE III: Parameters of Battery Storage Devices

$\mathbf{SoC}_{\min}$	$\mathbf{SoC}_{\max}$	η_b	$\lvert\bar{P}_b\rvert$ [GW]	E_b [GWh]
20%	80%	0.9	5	15

battery energy storage since more damping can be supplied by the storage system when the wind power is insufficient, therefore no need of load shedding.

It should be noted that although battery energy storage system could reduce the total operation cost for balancing generation and demand, it is not reflected in this figure since the cost increment is always obtained by comparing with the case where no attack would occur.

VI. Conclusion and Future Work

A cyber-resilient economic dispatch model is proposed in this paper. The effectiveness of the proposed CRED is demonstrated through dynamic simulations. Case studies also illustrate the benefit and essential to consider the LAA parameter estimation. The LAAs have larger impact on system stability in systems with high wind penetration. The operation cost increment to maintain system stability is also influenced by the SI provision from wind turbines and the energy storage in the system. As a follow-up of this work we are looking at 1) the impact of time delay in attack detection and using more advanced and flexible defense strategies and 2) the influence of varying the droop gain of IBRs on the converter-driven instability in weak grids.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2009, pp. 21–32.

[2] F. Bellizio, W. Xu, D. Qiu, Y. Ye, D. Papadaskalopoulos, J. L. Cremer, F. Teng, and G. Strbac, "Transition to digitalized paradigms for security control and decentralized electricity market," *Proceedings of the IEEE*, pp. 1–18, 2022.

[3] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 635–646, 2021.

[4] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proc. Annual Computer Security Applications Conference (ACSAC)*, 2017, pp. 303–314.

[5] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. USENIX Security*, 2018, pp. 15–32.

[6] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in *Proc. USENIX Security Symposium*, Aug. 2019, pp. 1115–1132.

[7] J. Ospina *et al.*, "On the feasibility of load-changing attacks in power systems during the covid-19 pandemic," *IEEE Access*, vol. 9, pp. 2545–2563, 2021.

[8] S. Lakshminarayana, J. Ospina, and C. Konstantinou, "Load-altering attacks against power grids under COVID-19 low-inertia conditions," *IEEE Open Access Journal of Power and Energy*, pp. 1–1, 2022. [Online]. Available: 10.1109/OAJPE.2022.3155973

[9] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, July 2018.

[10] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[11] S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of iot-based load altering attacks against power grids using the theory of second-order dynamical systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4415–4425, 2021.

[12] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Detecting dynamic load altering attacks: A data-driven time-frequency analysis," in *Proc. SmartGridComm*, 2015, pp. 503–508.

[13] S. Amini, F. Pasqualetti, M. Abbaszadeh, and H. Mohsenian-Rad, "Hierarchical location identification of destabilizing faults and attacks in power systems: A frequency-domain approach," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2036–2045, 2019.

[14] M. Izbicki, S. Amini, C. R. Shelton, and H. Mohsenian-Rad, "Identification of destabilizing attacks in power systems," in *Proc. American Control Conference (ACC)*, 2017, pp. 3424–3429.

[15] S. Lakshminarayana, S. Sthapit, H. Jahangir, C. Maple, and H. V. Poor, "Data-driven detection and identification of iot-enabled load-altering attacks in power grids," *IET Smart Grid*, pp. 1–16, 2022. [Online]. Available: https://doi.org/10.1049/stg2.12066

[16] S. Soltan, P. Mittal, and H. V. Poor, "Protecting the grid against mad attacks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 1310–1326, 2020.

[17] B. Shrestha and H. Lin, "Data-centric edge computing to defend power grids against iot-based attacks," *Computer*, vol. 53, no. 5, pp. 35–43, 2020.

[18] C. Chen, M. Cui, X. Fang, B. Ren, and Y. Chen, "Load altering attack-tolerant defense strategy for load frequency control system," *Applied Energy*, vol. 280, p. 116015, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261920314586

[19] Y. Guo, L. Wang, Z. Liu, and Y. Shen, "Reinforcement-learning-based dynamic defense strategy of multistage game against dynamic load altering attack," *International Journal of Electrical Power & Energy Systems*, vol. 131, p. 107113, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061521003525

[20] Z. Chu and F. Teng, "Short circuit current constrained uc in high ibg-penetrated power systems," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3776–3785, 2021.

[21] L. Huang, H. Xin, Z. Li, P. Ju, H. Yuan, Z. Lan, and Z. Wang, "Grid-synchronization stability analysis and loop shaping for pll-based power converters with different reactive power control," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 501–516, 2020.

[22] Z. Chu, N. Zhang, and F. Teng, "Frequency-constrained resilient scheduling of microgrid: A distributionally robust approach," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[23] Y. Fang, K. Jia, Z. Yang, Y. Li, and T. Bi, "Impact of inverter-interfaced renewable energy generators on distance protection and an improved scheme," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 9, pp. 7078–7088, 2019.

[24] Hatziargyriou, Nikos *et al.*, "Definition and classification of power system stability – revisited & extended," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3271–3281, 2021.

[25] S. D'Arco and J. A. Suul, "Equivalence of virtual synchronous machines and frequency-droops for converter-based microgrids," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 394–395, 2014.

[26] U. Markovic, Z. Chu, P. Aristidou, and G. Hug, "Lqr-based adaptive virtual synchronous machine for power systems with high inverter penetration," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 3, pp. 1501–1512, 2019.

[27] G. C. Calafiore and L. E. Ghaoui, "On distributionally robust chance-constrained linear programs," *Journal of Optimization Theory and Applications*, pp. 1–22, 2006.

[28] Z. Chu, U. Markovic, G. Hug, and F. Teng, "Towards optimal system scheduling with synthetic inertia provision from wind turbines," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 4056–4066, 2020.

[29] F. Teng, V. Trovato, and G. Strbac, "Stochastic scheduling with inertia-dependent fast frequency response requirements," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1557–1566, 2016.

[30] A. Moeini, I. Kamwa, P. Brunelle, and G. Sybille, "Open data ieee test systems implemented in simpowersystems for education and research in power grid dynamics and control," in *2015 50th International Universities Power Engineering Conference (UPEC)*, 2015, pp. 1–6.

[31] Grigg, C *et al.*, "The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 1010–1020, 1999.

[32] "Met Office. Weather Forecasts," 2022, accessed: 2022-5-18. [Online]. Available: https://www.metoffice.gov.uk/public/weather