Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.074277

ARTICLE

Detecting and Mitigating Cyberattacks on Load Frequency Control with Battery Energy Storage System

Yunhao Yu[1], **Fuhua Luo**[1] **and Zhenyong Zhang**[2,*]

[1]Electric Power Dispatching and Control Center, Guizhou Power Grid Co., Ltd., Guiyang, 550002, China
[2]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, 550025, China

*Corresponding Author: Zhenyong Zhang. Email: zyzhangnew@gmail.com

Received: 07 October 2025; Accepted: 26 November 2025; Published: 10 February 2026

ABSTRACT: This paper investigates the detection and mitigation of coordinated cyberattacks on Load Frequency Control (LFC) systems integrated with Battery Energy Storage Systems (BESS). As renewable energy sources gain greater penetration, power grids are becoming increasingly vulnerable to cyber threats, potentially leading to frequency instability and widespread disruptions. We model two significant attack vectors: load-altering attacks (LAAs) and false data injection attacks (FDIAs) that corrupt frequency measurements. These are analyzed for their impact on grid frequency stability in both linear and nonlinear LFC models, incorporating generation rate constraints and nonlinear loads. A coordinated attack strategy is presented, combining LAAs and FDIAs to achieve stealthiness by concealing frequency deviations from system operators, thereby maximizing disruption while evading traditional detection. To counteract these threats, we propose an Unknown Input Observer (UIO)-based detection framework for linear and nonlinear LFCs. The UIO is designed using linear matrix inequalities (LMIs) to estimate system states while isolating unknown attack inputs, enabling attack detection through monitoring measurement residuals against a predefined threshold. For mitigation, we leverage BESS capabilities with two adaptive strategies: dynamic mitigation for dynamic LAAs, which tunes BESS parameters to enhance the system's stability margin and accelerate convergence to equilibrium; and static mitigation for static LAAs and FDIAs. Simulations show that the UIO achieves high detection accuracy, with residuals exceeding thresholds promptly under coordinated attacks, even in nonlinear models. Mitigation strategies reduce frequency deviations by up to 80% compared to unmitigated cases, restoring stability within seconds.

KEYWORDS: Load frequency control; cybersecurity; unknown input observer; battery energy storage system

1 Introduction

The reliable operation of modern power grids is critically dependent on Load Frequency Control (LFC) systems, which maintain the balance between power generation and demand, thereby ensuring stable grid frequency [1]. However, the increasing complexity and interconnectivity of power systems, particularly with the growing integration of renewable energy sources and advanced communication infrastructures, have exposed them to new vulnerabilities, including cyberattacks [2]. These cyber threats pose significant risks to grid stability, potentially leading to widespread blackouts and economic disruption.

Cyberattacks on LFC systems can manifest in various forms, such as false data injection (FDI) into sensor measurements or control commands [3,4], and load-altering attacks (LAA) [5,6] that manipulate demand-side parameters. These attacks can deceive control systems, leading to incorrect control actions, frequency excursions, and ultimately, system instability. The challenge lies not only in detecting such sophisticated attacks but also in mitigating their impact effectively and rapidly to maintain grid resilience. FDI attacks have been widely studied as a means to manipulate sensor measurements or control signals in LFC, leading to frequency deviations [7]. For instance, optimal FDIA schemes against automatic generation control (AGC) in LFC have been analyzed to disrupt frequency regulation [8]. Load-altering attacks (LAAs), including dynamic and static variants, have also been investigated for their ability to create generation-load imbalances [9].

Detection techniques often leverage observers or data-driven approaches. Unknown input observers (UIOs) have proven effective for detecting cyberattacks in large-scale power systems by estimating states while isolating unknown disturbances [10]. Specifically for LFC, UIOs have been applied to detect attacks on tie-line power in multi-area systems and to enable secure state estimation under sparse sensor attacks [11]. Sliding mode observers and Kalman filters combined with UIOs have been proposed for robust detection in power grids [12,13]. Data-driven methods, including deep reinforcement learning for attack detection in LFC and machine learning for hybrid cyberattacks in power grids, offer alternatives to model-based approaches [14,15].

Mitigation strategies frequently incorporate energy storage systems. Battery Energy Storage Systems (BESS) have been utilized for frequency control in renewable grids under cyberattacks [16]. Defense mechanisms against LAAs in LFC include tolerant control strategies that adjust system parameters to maintain stability [17]. Reviews highlight the implementation, detection, and mitigation of cyberattacks, emphasizing the role of BESS in enhancing resilience [18].

While prior work has advanced UIO-based detection for FDIAs or LAAs individually, few address coordinated scenarios in which dynamic load-altering attacks (DLAAs), static load-altering attacks (SLAAs), and FDIAs are combined to achieve stealth by concealing frequency deviations. Existing UIO applications in LFC are often limited to linear models and multi-area tie-line attacks, whereas data-driven methods may require extensive training data and lack interpretability for real-time operation. Mitigation via BESS in previous studies focuses on general frequency regulation under hybrid attacks. Still, it does not explicitly tune BESS parameters or inject power adaptively for coordinated attack recovery, nor does it extend to nonlinear LFC models incorporating generation rate constraints or nonlinear loads. In contrast, this paper integrates UIO detection with BESS mitigation in a unified framework, addressing stealthy coordinated attacks and nonlinearities to improve robustness [19].

This paper addresses the critical issue of detecting and mitigating coordinated cyberattacks on LFC systems augmented with BESS. Our key contributions are as follows: (1) We model a stealthy coordinated attack scenario combining DLAAs, SLAAs, and FDIAs, designed to maximize disruption while evading detection by concealing frequency deviations; (2) We propose a UIO-based approach for attack detection, extended to both linear and nonlinear LFC models, enabling state estimation and residual monitoring even in the presence of unknown attack signals; (3) We develop BESS-enabled mitigation strategies, including dynamic tuning of BESS parameters for DLAAs and static power injection for SLAAs and FDIAs, to rapidly restore frequency stability; (4) Through simulations on real load data, we validate the UIO's detection accuracy and the BESS's mitigation efficacy, demonstrating enhanced resilience against sophisticated cyber threats in LFC systems.

2 Load Frequency Control with the Battery Energy Storage System

Here, we introduce the load frequency control (LFC) with the battery energy storage system (BESS). The function of the LFC is to balance the power load and generation, thereby maintaining the grid frequency at its nominal value (e.g., 50 or 60 Hz). The BESS is a quick-acting module that compensates for the generator's response to frequency variations. It detects frequency deviation and rapidly injects power into the grid (in the event of a shortage) or absorbs power (in the event of an excess) to counteract the imbalance. BESS has the potential to address the stability issues caused by increasing penetration of renewable energy sources. In this paper, the BESS is integrated into the system to provide primary frequency control reserves. As shown in Fig. 1, the primary and the secondary control are given with respect to the frequency deviation. For more details, the formal descriptions are given as follows. The primary control with BESS is

$$\dot{\Delta f} = -\frac{-D}{2R}\Delta f + \frac{1}{2R}\Delta P_G + \frac{1}{2R}\Delta P_B - \frac{1}{2R}\Delta P_L, \Delta\dot{P}_G = -\frac{1}{T_G H_G}\Delta f - \frac{1}{T_G}\Delta P_G - \frac{1}{T_G}\Delta F_O, \tag{1}$$

$$\Delta\dot{P}_B = -\frac{1}{T_B H_B}\Delta f - \frac{1}{T_B}\Delta P_B, \tag{2}$$

where $\dot{\Delta f}$ is the rate of the frequency deviation, D is the damping ratio of the generation system, R is the power system inertia, Δf is the frequency deviation, ΔP_G is the output deviation of the mechanical power, ΔP_B is the output deviation of the battery energy, ΔP_L is the deviation of the power load, T_G and T_B are the power system and BESS time constants, respectively, ΔF_O is the reference of the frequency deviation, which is determined by the secondary frequency control, and H_G and H_B are the droop gains of the generator and BESS, respectively. The secondary frequency control is designed in a proportional form, that is, $\Delta F_O = K_P \Delta f$, where K_P is the proportional factor for generating the frequency reference.

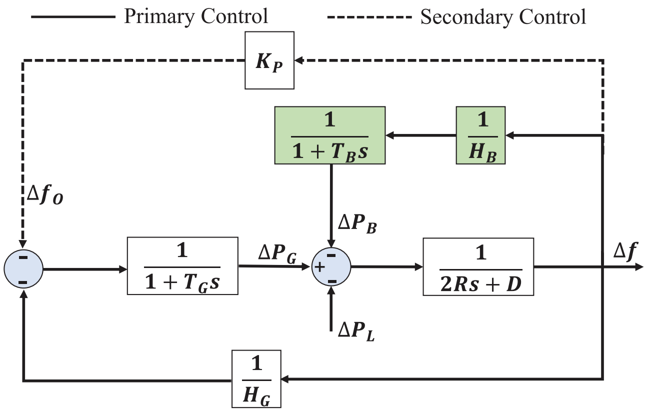


Figure 1: The diagram of the LFC with BESS

To be concise, we rewrite system model in state-space form. By letting $\mathbf{x} = [\Delta f, \Delta P_G, \Delta P_B]^T$ and $\mathbf{u} = [\Delta P_L, \Delta F_O]$, we have

$$\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u}, \mathbf{y} = C\mathbf{x}, \tag{3}$$

where $A = \begin{bmatrix} -\frac{D}{2R} & \frac{1}{2R} & \frac{1}{2R} \\ -\frac{1}{T_G H_G} & -\frac{1}{T_G} & 0 \\ -\frac{1}{T_B H_B} & 0 & -\frac{1}{T_B} \end{bmatrix}$, $B = \begin{bmatrix} -\frac{1}{2R} & 0 \\ 0 & -\frac{1}{T_G} \\ 0 & 0 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$. Then, we have $\mathbf{u} = \begin{bmatrix} 0 \\ K_P \end{bmatrix}\mathbf{y}$. It indicates that the secondary control has an output feedback controller. The frequency deviation is controlled to 0 with load variation.

3 Coordinated Attack on the LFC

However, because it relies on information and communication infrastructure, load frequency control is vulnerable to cyberattacks. Since the load is on the user's side, the load measurement can be manipulated, allowing the actual load to be maliciously altered. The secondary control requires communication between the field site and the control center, creating opportunities for attackers to corrupt measurements and control commands. The attack scenarios are given in Fig. 2.

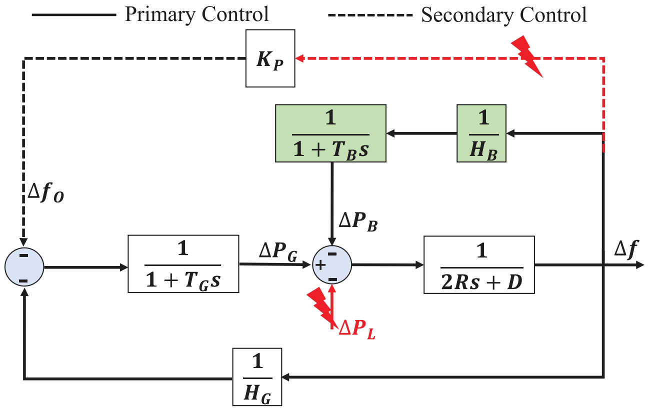


Figure 2: The attack on the LFC with BESS

3.1 Load Altering Attack

First, for the load, suppose it can be modelled with the frequency-sensitive and static loads, that is, $\Delta P_L = \beta * \Delta f + L_0$, where $\beta \geq 0$ and L_0 is the static load. Therefore, there are two types of load-altering attacks: dynamic load-altering attacks (DLAAs) and static load-altering attacks (SLAAs). The DLAA is modeled as

$$\Delta \tilde{P}_L = \beta * \Delta f + L_0 + a\Delta f = (\beta + a)\Delta f + L_0, \tag{4}$$

where a is the attack coefficient for the frequency-sensitive load. The SLAA is modeled as

$$\Delta P_L = \beta * \Delta f + L_0 + L_a, \tag{5}$$

where L_a is the maliciously injected frequency-insensitive load. The joint attack of DLAA and SLAA is modeled as

$$\Delta P_L = (\beta + a) * \Delta f + L_0 + L_a. \tag{6}$$

The load-altering attack can cause a generation-load imbalance, leading to frequency variation and potentially an unstable system.

3.2 False Data Injection Attack

Second, the frequency measurement can be compromised in the communication network. That is, the false data injection attack (FDIA) is executed by injecting an error into the frequency deviation. The FDIA can be modeled as

$$\tilde{\mathbf{y}} = \mathbf{y} + \mathbf{y}^a, \tag{7}$$

where $\mathbf{y}^a$ is error injected by the FDIA. Due to the output feedback control, the FDIA can affect the frequency stability.

3.3 *Coordinated Attack*

In some cases, the attacker is powerful and can carry out a coordinated attack. For example, the attack on the Ukrainian power grid in 2015 was a typical coordinated attack, executing cyberattacks in a perfectly organized manner at specific locations to maximize the impact on the system's operation [20]. In our scenario, the load-altering attack and FDIA can be coordinated to make the attack stealthy. The coordinated attack can be modeled as

$$\begin{bmatrix} \Delta\dot{f} \\ \Delta\dot{P}_G \\ \Delta\dot{P}_B \end{bmatrix} = \begin{bmatrix} -\dfrac{D}{2R} & \dfrac{1}{2R} & \dfrac{1}{2R} \\ -\dfrac{1}{T_G H_G} & -\dfrac{1}{T_G} & 0 \\ -\dfrac{1}{T_B H_B} & 0 & -\dfrac{1}{T_B} \end{bmatrix} \begin{bmatrix} \Delta f \\ \Delta P_G \\ \Delta P_B \end{bmatrix} + \begin{bmatrix} -\dfrac{1}{2R} & 0 \\ 0 & -\dfrac{1}{T_G} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} (\beta + a)\Delta f + L_0 + L_a \\ K_P(\Delta f + \mathbf{y}^a) \end{bmatrix} \tag{8}$$

Furthermore, we can derive that

$$\begin{bmatrix} \Delta\dot{f} \\ \Delta\dot{P}_G \\ \Delta\dot{P}_B \end{bmatrix} = \begin{bmatrix} -\dfrac{D + \beta + a}{2R} & \dfrac{1}{2R} & \dfrac{1}{2R} \\ -\dfrac{K_P}{T_G H_G} & -\dfrac{1}{T_G} & 0 \\ -\dfrac{1}{T_B H_B} & 0 & -\dfrac{1}{T_B} \end{bmatrix} \begin{bmatrix} \Delta f \\ \Delta P_G \\ \Delta P_B \end{bmatrix} + \begin{bmatrix} -\dfrac{1}{2R} & 0 \\ 0 & -\dfrac{1}{T_G} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} L_0 + L_a \\ K_P\mathbf{y}^a \end{bmatrix} \tag{9}$$

The stealthiness of the coordinated attack is achieved by using $\mathbf{y}^a$ to conceal the frequency deviation. From the system operator's angle, the frequency deviation is always at zero or a controlled level.

4 Attack Detection with the Unknown Input Observer

The attacks introduced in Section 3 pose a serious threat to the system's normal operation. The unexpected distortions cause the LFC to fail to maintain generation-load balance, leading to frequency excursions and potentially destabilizing the grid. Therefore, it is crucial to identify and capture this abnormal behavior. Considering the attacks as unknown inputs, we aim to design an unknown-input observer (UIO) to detect them. The system model with the unknown attack is given as

$$\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u} + E\mathbf{v}, \mathbf{y} = C\mathbf{x}. \tag{10}$$

Since the power load changes with a lot of uncertainties, the Δf as a whole is treated as an unknown term. The input $\mathbf{u}$ is given as $\mathbf{u} = \Delta F_O$ and the matric B is $B = \begin{bmatrix} 0 \\ -\dfrac{1}{T_G} \\ 0 \end{bmatrix}$. The matrix E is $E = \begin{bmatrix} -\dfrac{1}{2R} & 0 \\ 0 & -\dfrac{1}{T_G} \\ 0 & 0 \end{bmatrix}$. The load-altering attack and the FDIA on the frequency deviation are treated as the unknown term.

Considering a full-order UIO [21], the observer proposed for detecting attacks is given by the following structure. That is, we have

$$\dot{\mathbf{z}} = N\mathbf{z} + W\mathbf{u} + Q\mathbf{y}, \hat{\mathbf{x}} = \mathbf{z} - S\mathbf{y}, \tag{11}$$

where $\mathbf{z}$ is the UIO state vector, N, W, and Q are matrices that should be carefully designed to estimate the state, i.e., $\hat{\mathbf{x}}$, ignoring the unknown inputs. These four matrices are defined as

$$N = XA - VC, W = XB, X = I + SC, Q = V(I + CS) - XAS, \tag{12}$$

where S and V should be designed for the UIO. With the UIO, the state estimation error is

$$\mathbf{e} = \hat{\mathbf{x}} - \mathbf{x} = z - S\mathbf{y} - \mathbf{x} = z - (I + SC)\mathbf{x} = z - X\mathbf{x}. \tag{13}$$

Taking the derivative of the estimation error, we have

$$\dot{\mathbf{e}} = N\mathbf{e} + (NX + QC - XA)\mathbf{x} + (W - XB)\mathbf{u} - XE\mathbf{v} \tag{14}$$

Therefore, we can obtain that

$$W - XB = 0, NX + QC - XA = 0. \tag{15}$$

The latter can be derived as

$$\begin{aligned} NX + QC - XA &= NX + (V(I + CS) - XAS)\,C - XA = NX + VC + VCSC - XASC - XA \\ &= NX + VC - NSC - XA = N + NSC + VC - NSC - XA = 0 \end{aligned} \tag{16}$$

Next, a sufficient condition is provided to prove the existence of the UIO.

Lemma 1. *There exists a UIO for the unknown input system (10) if there exist S and V and a positive definite symmetric matrix $P > 0$ such that $SCE = -E, N^T P + PN < 0$.*

Proof: Based on the above derivations, we have $\dot{\mathbf{e}} = N\mathbf{e} - XE\mathbf{v}$. Since $SCE = -E$, we can derive that $XE = (I + SC)E = 0$. Therefore, we have $\dot{\mathbf{e}} = N\mathbf{e}$. According to the Lyapunov stability theory [22], if there exists a positive definite symmetric matrix $P > 0$ such that $N^T P + PN < 0$, the estimation error $\mathbf{e}$ goes to 0 asymptotically for any initial value of $\mathbf{e}$. □

Therefore, with the conditions given in Lemma (1), the UIO accurately estimates the system state without knowing the input $\mathbf{v}$. Next, we need to solve for the matrices S and V to design the UIO. As for S, since the matrix E is of full column rank, the equation $SCE = -E$ can be solved only if the matrix SC is also of full column rank. Suppose the matrix SC is of full column rank, then the matrix E is obtained by

$$S = -E(CE)^+ + Y\left(I - (CE)(CE)^+\right), \tag{17}$$

where $(CE)^+ = ((CE)^T(CE))^{-1}(CE)^T$ and Y is an arbitrarily matrix. To be concise, we have $S = U + YZ$, where $U = -E(CE)^+$ and $Z = I - (CE)(CE)^+$. Furthermore, we have

$$((I + UC)A)^T P + (ZCA)^T Y^T P - C^T V^T P + P(I + UC)A + PY(ZCA) - PVC < 0. \tag{18}$$

Therefore, solving the S, V, and $P > 0$ is equivalent to the problem of solving the inequality (18) with respect to Y, V, and $P > 0$. This matrix inequality can be formulated as an LMI. The LMI is usually given by $\begin{bmatrix} J & * \\ * & -I \end{bmatrix} < 0$, where $J = ((I+UC)A)^T P + P(I+UC)A + (ZCA)^T \bar{Y}^T + \bar{Y}(ZCA) - C^T \bar{V}^T - \bar{V}C$, $*$ means a zero matrix. Solving the LMI is equivalent to solve the matrix inequality (18) by making $Y = P^{-1}\bar{Y}$ and $V = P^{-1}\bar{V}$.

Above all, the algorithm for designing the UIO is given in Algorithm 1. With the designed UIO, the attacks are detected by monitoring the measurement residual $\mathbf{r} = \mathbf{y} - C\hat{\mathbf{x}}$. If the norm of the residual $\|\mathbf{r}\|$ is larger than a predefined threshold, then the attack is detected.

Algorithm 1: Design of the UIO

```
function UIO($A$, $B$, $C$, $E$)
    Compute $U = -E(CE)^+$ and $Z = I - (CE)(CE)^+$
    Solve the LMI for $\bar{Y}$, $\bar{V}$, and $P$.
    Obtain $Y = P^{-1}\bar{Y}$ and $V = P^{-1}\bar{V}$
    Compute
        $S = U + YZ, X = I + SC, N = XA - VC,$
        $G = XB, Q = V(I + CS) - XAS \quad (19)$
end function
```

Discussion. In our paper, the LMIs are solved offline during the UIO design phase to determine fixed matrices such as S, V, and P, which are then used to compute the observer gains N, W, and Q. Once designed, the real-time operation of the UIO involves only simple matrix-vector multiplications on a low-dimensional system (3 states for our single-area LFC model), which is computationally lightweight and executes in microseconds on standard hardware, well within LFC sampling intervals. For the offline LMI solving, modern solvers like MATLAB's LMI Toolbox or CVX handle small-scale problems (e.g., 3 × 3 matrices) efficiently, often in under 10 milliseconds on a standard CPU, as polynomial-time algorithms (e.g., interior-point methods) scale well for such dimensions. For context, larger LMIs in power system applications (e.g., with thousands of variables) have been reported to solve in minutes, but our case is negligible.

5 Mitigation of the Attacks with BESS

Once the attack is detected, mitigation measures should be implemented to reduce its impact. Here, the BESS is used to counteract the cyberattacks. There are two strategies to defend against the load-altering attacks and FDIA.

5.1 Dynamic Mitigation

Considering the DLAA only, from (9), we have

$$\begin{bmatrix} \Delta\dot{f} \\ \Delta\dot{P}_G \\ \Delta\dot{P}_B \end{bmatrix} = \begin{bmatrix} -\dfrac{D+\beta+a}{2R} & \dfrac{1}{2R} & \dfrac{1}{2R} \\ -\dfrac{K_P}{T_G H_G} & -\dfrac{1}{T_G} & 0 \\ -\dfrac{1}{T_B H_B} & 0 & -\dfrac{1}{T_B} \end{bmatrix} \begin{bmatrix} \Delta f \\ \Delta P_G \\ \Delta P_B \end{bmatrix} + \begin{bmatrix} -\dfrac{1}{2R} \\ 0 \\ 0 \end{bmatrix} L_0. \tag{20}$$

Concisely, we can rewrite (20) as

$$\dot{\mathbf{x}} = \tilde{A}\mathbf{x} + \tilde{B}L_0. \tag{21}$$

The system modes of (21) depend on the matrix $\tilde{A}$. The eigenvalues of $\tilde{A}$ determine the stability margin of the system (21). The DLAA with the parameter a changes the eigenvalues of $\tilde{A}$. The stability margin might also be changed. Suppose the eigenvalues of $\tilde{A}$ are $\tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3, \cdots, \tilde{\lambda}_n$. Then the stability margin is defined as $\theta = \sum_{i=1}^{n} \mathrm{Real}(\tilde{\lambda}_i)$. If the stability margin θ is smaller, the system is more stable and converges to the stable state faster. The BLAA can change the value of θ.

With BESS, the parameters T_B and H_B are tunable, as they are virtual indicators when treating the BESS as a generator. Actually, T_B and H_B are derived from the BESS's response rate to load changes. Suppose the stability margin after the DLAA is θ^{DLAA}. If the UIO detects the DLAA, the BESS parameters T_B and H_B can be tuned to mitigate it. After the mitigation, the stability margin is θ^{BESS}. Then, the mitigation strategy is effective only if $\theta^{\mathrm{BESS}} < \theta^{\mathrm{DLAA}}$.

5.2 Static Mitigation

Considering the SLAA and FDIA, from (9), we have

$$\begin{bmatrix} \dot{\Delta f} \\ \Delta\dot{P}_G \\ \Delta\dot{P}_B \end{bmatrix} = \begin{bmatrix} -\dfrac{D+\beta}{2R} & \dfrac{1}{2R} & \dfrac{1}{2R} \\ -\dfrac{K_P}{T_G H_G} & -\dfrac{1}{T_G} & 0 \\ -\dfrac{1}{T_B H_B} & 0 & -\dfrac{1}{T_B} \end{bmatrix} \begin{bmatrix} \Delta f \\ \Delta P_G \\ \Delta P_B \end{bmatrix} + \begin{bmatrix} -\dfrac{1}{2R} & 0 \\ 0 & -\dfrac{1}{T_G} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} L_0 + L_a \\ K_P \mathbf{y}^a \end{bmatrix}. \tag{22}$$

The BESS can mitigate the attack by injecting energy into the system. As shown in Fig. 3, the power is injected to balance the unexpected load and the modified measurement (which results in a wrong frequency reference). With the mitigation strategy, we can derive that

$$\begin{bmatrix} \dot{\Delta f} \\ \Delta\dot{P}_G \\ \Delta\dot{P}_B \end{bmatrix} = \begin{bmatrix} -\dfrac{D+\beta}{2R} & \dfrac{1}{2R} & \dfrac{1}{2R} \\ -\dfrac{K_P}{T_G H_G} & -\dfrac{1}{T_G} & 0 \\ -\dfrac{1}{T_B H_B} & 0 & -\dfrac{1}{T_B} \end{bmatrix} \begin{bmatrix} \Delta f \\ \Delta P_G \\ \Delta P_B \end{bmatrix} + \begin{bmatrix} -\dfrac{1}{2R} & 0 & 0 \\ 0 & -\dfrac{1}{T_G} & 0 \\ 0 & 0 & -\dfrac{1}{T_B} \end{bmatrix} \begin{bmatrix} L_0 + L_a \\ K_P \mathbf{y}^a \\ \Delta P_E \end{bmatrix}, \tag{23}$$

where ΔP_E is the injected battery power. It is calculated based on an estimate of the attack magnitudes L_a (for SLAAs) or y^a (for FDIAs), derived from reconstructing the unknown input v (which encapsulates these attacks). Specifically, after detection via the residual $\|r\| >$ threshold, we estimate v using the UIO's state estimates $\hat{x}$ as $\hat{v} = (E^T E)^{-1} E^T(\dot{\hat{x}} - A\hat{x} - Bu)$, where $\dot{\hat{x}}$ is approximated from the observer dynamics. Then, ΔP_E is set proportionally to the relevant component of $\hat{v}$ (e.g., $-\frac{1}{2R}L_a$ or $-\frac{K_P}{T_G}y^a$) to balance the induced distortion and restore the generation-load equilibrium. This estimation makes the mitigation feedback-based rather than purely open-loop, enhancing robustness against uncertainties in attack parameters. However, to address potential inaccuracies in $\hat{v}$ (e.g., due to noise), we can periodically re-estimate and adjust ΔP_E in real-time, forming an adaptive loop.

6 UIO with the Nonlinear LFC

In Section 2, we consider a linear model for the LFC. However, there are nonlinearities in the generator and BESS. Therefore, the designed UIO should be extended to the nonlinear case. The unknown input is the attack presented in Section 3. In the following, we present two examples of nonlinearity.

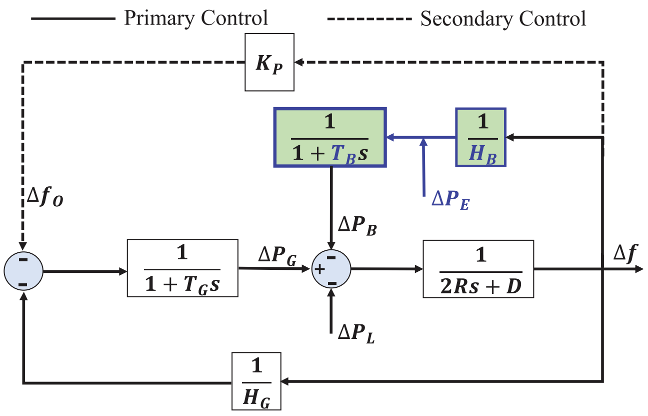


Figure 3: The attack mitigation with BESS

In case 1, the generation rate constraint (GRC) is considered. The GRC limits changes in generation power. This is a saturation nonlinearity on the derivative of ΔP_G. The nonlinearity can be modeled as

$$\Delta \dot{P}_G = -\frac{1}{T_G H_G}\Delta f + \text{sat}(-\frac{1}{T_G}\Delta P_G, \text{GRC}) - \frac{1}{T_G}\Delta F_O, \tag{24}$$

where

$$\text{sat}(x, \text{GRC}) = \begin{cases} x & \text{if } |x| \le \text{GRC} \\ \text{GRC} * \text{sign}(x) & \text{otherwise} \end{cases} \tag{25}$$

where sign(x) computes the sign of x.

In case 2, the load consists of a frequency-sensitive nonlinear component. That is, the load is modeled as $\Delta P_L = \beta_1 \Delta f + \beta_2(\Delta f)^2 + L_0$. Considering these nonlinearities, in a concise way, the system dynamics is modeled as

$$\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u} + f(\mathbf{x}) + E\mathbf{v}, \dot{\mathbf{y}} = C\mathbf{x}. \tag{26}$$

In different nonlinear cases, the matrices A, B, and E might be different. However, the UIO is designed in a general form. The structure of the UIO is

$$\dot{\mathbf{z}} = N\mathbf{z} + W\mathbf{u} + Q\mathbf{y} + Mf(\hat{\mathbf{x}}), \hat{\mathbf{x}} = z - S\mathbf{y}. \tag{27}$$

The matrices N, W, Q, and M are matrices that should be designed for the UIO. They are defined by $N = MA - VC$, $W = MB$, $M = I + SC$, $Q = V(I + CS) - MAS$. Therefore, we can derive the state estimation error as $\dot{\mathbf{e}} = N\mathbf{e} + (NM + QC - MA)\mathbf{x} + (W - MB)\mathbf{u} + M\,(f(\hat{\mathbf{x}} - f(\mathbf{x})) - ME\mathbf{v}$.

From the three nonlinear cases, we can easily derive that

$$|f(\mathbf{x}) - f(\hat{\mathbf{x}})| \le \eta|\mathbf{x} - \hat{\mathbf{x}}|, \tag{28}$$

where $\eta > 0$. Next, we present the condition for the existence of the UIO with nonlinear terms.

Lemma 2. *There exists a UIO for the unknown input system (10) if there exist S and V and a positive definite symmetric matrix $P > 0$ such that $SCE = -E, N^T P + PN + \eta PMM^T P + \eta I < 0$.*

Proof: We can derive that $W - MB = 0$ and $NX + QC - XA = 0$. Therefore, we can obtain that $\dot{\mathbf{e}} = N\mathbf{e} + M\left(f(\hat{\mathbf{x}}) - f(\mathbf{x})\right) - ME\mathbf{v}$. The condition $SCE = -E$ implies that $ME = 0$, and we have $\dot{\mathbf{e}} = N\mathbf{e} + M\left(f(\hat{\mathbf{x}}) - f(\mathbf{x})\right)$. By choosing a Lyapunov function as $G = \mathbf{e}^T P\mathbf{e}$, we can derive that

$$\begin{aligned}\dot{G} &= \mathbf{e}^T(N^TP + PN)\mathbf{e} + 2\mathbf{e}^TPM\left(f(\hat{\mathbf{x}}) - f(\mathbf{x})\right) \le \mathbf{e}^T(N^TP + PN)\mathbf{e} + 2\|\mathbf{e}^TPM\|\|f(\hat{\mathbf{x}}) - f(\mathbf{x})\| \\ &\le \mathbf{e}^T(N^TP + PN)\mathbf{e} + 2\eta\|\mathbf{e}^TPM\|\|\mathbf{e}\| \le \mathbf{e}^T(N^TP + PN)\mathbf{e} + \eta(\|\mathbf{e}^TPM\|^2 + \|\mathbf{e}\|^2) \\ &= \mathbf{e}^T(N^TP + PN + \eta PMM^TP + \eta I)\mathbf{e} \end{aligned} \tag{29}$$

The condition $N^TP + PN + \eta PMM^TP + \eta I < 0$ indicates that $\mathbf{e}$ goes to 0 asymptotically for any initial value. Therefore, the UIO exists with the condition. □

With the Lemma 2, the matrices S, V, and P are computed according to the condition $N^TP + PN + \eta PMM^TP + \eta I < 0$. The possible solutions of S are obtained from $SCE = -E$. Therefore, the matrix E is of full column rank. The necessary condition for $SCE = -E$ to have solutions is that CE is also of full column rank. Hence, the matrix S is obtained by $S = -E(CE)^+ + Y\left(I - (CE)(CE)^+\right)$, where $(CE)^+ = ((CE)^T(CE))^{-1}(CE)^T$ and Y is an arbitrarily matrix. Furthermore, we have $S = U + Y Z$, where $U = -E(CE)^+$ and $Z = I - (CE)(CE)^+$. Next, we substitute S into $N^TP + PN + \eta PMM^TP + \eta I < 0$, we have

$$\begin{aligned}&((I + UC)A)^T P + (ZCA)^T Y^T P - C^T V^T P + P(I + UC)A + PY(ZCA) - PVC \\ &\qquad + \eta\left(P(I + UC) + PY(ZC)\right)\left(P(I + UC) + PY(ZC)\right)^T + \eta I < 0.\end{aligned} \tag{30}$$

Solving (30) for S, V, and P is an LMI problem. We can construct a matrix inequality as $\begin{bmatrix} J & \check{J} \\ \check{J}^T & -I \end{bmatrix} < 0$, where J is given by

$$\begin{aligned}J &= ((I + UC)A)^T P + P(I + UC)A + (ZCA)^T\bar{Y}^T + \bar{Y}(ZCA) - C^T\bar{V}^T - \bar{V}C + \eta I \\ \check{J} &= \sqrt{\eta}\left(P(I + UC) + \bar{Y}(ZC)\right),\end{aligned} \tag{31}$$

where $Y = P^{-1}\bar{Y}$ and $V = P^{-1}\bar{V}$. The LMI $\begin{bmatrix} J & \check{J} \\ \check{J}^T & -I \end{bmatrix} < 0$ is equivalent to $\begin{bmatrix} J + \check{J}\check{J}^T & * \\ * & -I \end{bmatrix} < 0$. Therefore, (30) is a sufficient condition for the existence of the UIO. With the above derivations, the Algorithm 2 is used to design the UIO.

Algorithm 2: Design of the UIO

```
function UIO($A, B, C, E$)
    Compute $U = -E(CE)^+$ and $Z = I - (CE)(CE)^+$
    Solve the LMI for $\bar{Y}$, $\bar{V}$, and $P$.
    Obtain $Y = P^{-1}\bar{Y}$ and $V = P^{-1}\bar{V}$
    Compute
        $S = U + YZ, M = I + SC, N = MA - VC,$
        $G = MB, Q = V(I + CS) - MAS$                (32)
end function
```

Discussion. The onlinearities are modeled as additive terms $f(x)$ in the system dynamics: $\dot{x} = Ax + Bu + f(x) + Ev$, where $f(x)$ satisfies a Lipschitz condition $|f(x) - f(\hat{x})| \leq \eta|x - \hat{x}|$ for some $\eta > 0$ (derived from the specific cases in Section 6, e.g., saturation in GRC or quadratic load components). For attack detection, the UIO is augmented to include $Mf(\hat{x})$ in its dynamics, and stability is ensured via a modified Lyapunov condition in Lemma 2 ($NTP + PN + \eta PMM^T P + \eta I < 0$), solved through an adapted LMI that incorporates the Lipschitz constant η. This allows the UIO to decouple unknown attacks (v) while bounding the impact of nonlinear terms, ensuring asymptotic convergence of the estimation error even in nonlinear scenarios.

7 Simulation Results

In this section, we conduct simulations to analyze the impact of the attack, the UIO's attack-detection performance, and the BESS's mitigation performance. All simulations are carried out in MATLAB (Simulink), and the computational device is a laptop equipped with an 11th Gen Intel(R) Core(TM) i7-1165G7 processor, operating at 2.80 GHz and featuring 32 GB of RAM. The system parameters are set to as $D = 0.8$ pu, $H_G = 0.05$ pu, $T_G = 0.2$ s, $H_B = 0.04$ pu, $T_B = 0.02$ s, and $R = 5$ s. The power load is extracted from the New York Independent System Operator (NYISO)[1]. Fig. 4 presents the load variation for the simulations, showing changes at 5, 10, and 15 s.

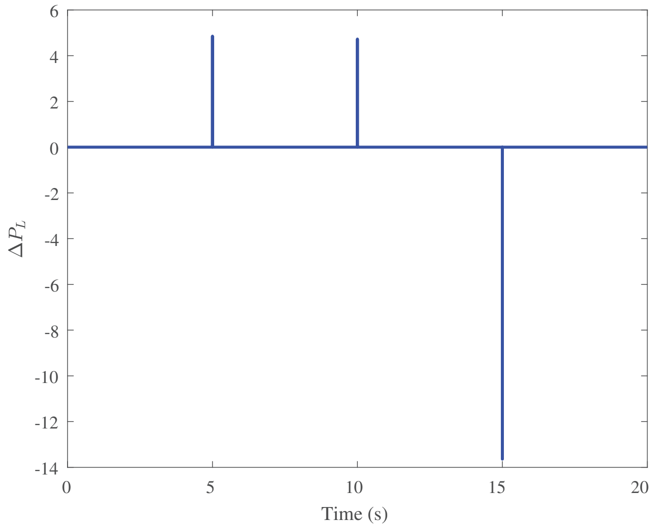


Figure 4: The power load variation

7.1 Attack on the LFC

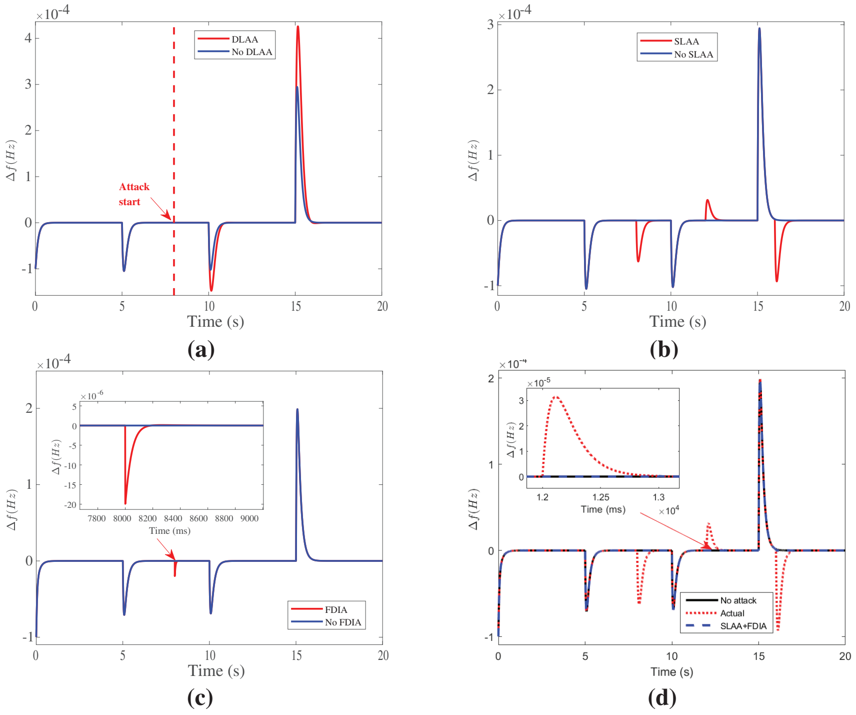
First, we analyze the impact of the attacks described in Section 3 on the grid frequency. The attack parameters are:

- DLAA: Only the DLAA is executed, the frequency-sensitive load coefficient is $\beta = 100$ and the attack parameter is $a = -60$. The attack starts at 8 s.
- SLAA: Only the SLAA is executed, the loads are injected at 8 s with $L_a = 2.91$ pu, at 12 s with $L_a = -1.45$ pu, and at 16 s with $L_a = -4.37$ pu.
- FDIA: Only the FDIA is executed, the measurement of the frequency deviation is modified with an error $\mathbf{y}^a = 0.002$ at 12 s.

[1] Load Data, https://www.nyiso.com/load-data (accessed on 23 November 2025).

- SLAA+FDIA: The SLAA and FDIA are coordinated. The attack parameters for SLAA remain unchanged, while the FDIA mitigates the attack's impact by injecting a measurement error.

The simulation results are given in Fig. 5. For the DLAA (Fig. 5a), we find that the magnitude of Δf is larger than that without DLAA, which indicates that the DLAA affects the convergence rate of the frequency deviation. That is, the DLAA causes the system to take more time to return to a stable state. For the SLAA (Fig. 5b), we find that the attack causes distortions for Δf from the stable state. That is, the SLAA causes the system to deviate from its normal state. For the FDIA (Fig. 5c), we find it also distorts Δf from the stable state. For the SLAA+FDIA (Fig. 5d), we find that the coordinated attack is stealthy because the frequency deviation Δf after SLAA+FDIA is the same as that without attack, while the actual Δf deviates from the normal state. Fig. 5d illustrates the stealthiness of the coordinated SLAA+FDIA attack. Here, the SLAA introduces a static load distortion (L_a), causing the actual frequency deviation Δf to excursion away from equilibrium, potentially leading to instability. However, the concurrent FDIA injects ya to falsify the measurement $\tilde{y}$, making the observed Δf appear stable and within nominal bounds from the system operator's viewpoint. The attacked measurement y_a counteracts the visible effects of L_a, allowing the attack to persist undetected without immediate alarms. The above results demonstrate that the attack can affect the system frequency, and different attacks have different impacts.



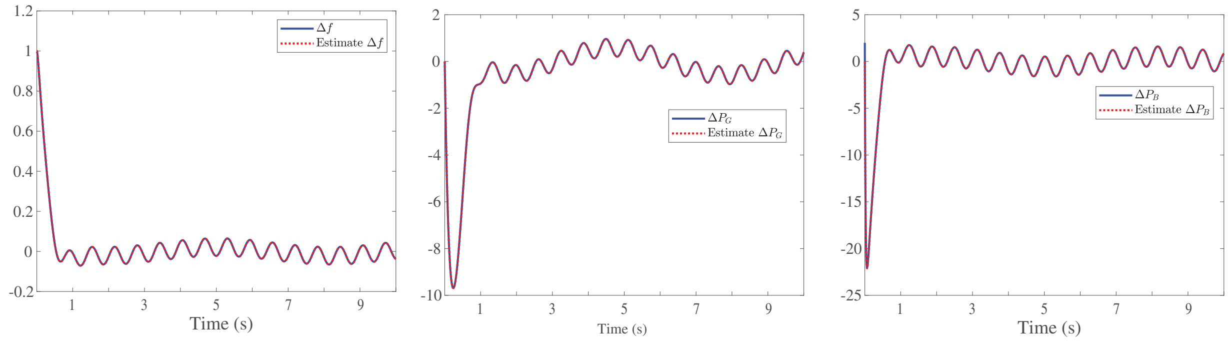
(a) (b) (c) (d)

Figure 5: Simulation results demonstrating the impact of various cyberattacks on grid frequency deviation (Δf). (**a**) Under DLAA, Δf exhibits rapid oscillations with peaks up to 0.05 Hz within 10 s due to dynamic load amplification tied to frequency. (**b**) SLAA causes sustained offsets of 0.03 Hz from static load distortions, leading to persistent imbalances. (**c**) FDIA induces erratic excursions by falsifying measurements, potentially destabilizing control actions. (**d**) Coordinated SLAA+FDIA demonstrates stealthiness: the actual Δf deviates significantly (up to 0.04 Hz). In contrast, the measured Δf appears controlled and near zero from the operator's perspective, masking the attack and allowing prolonged disruption. This figure shows the stealthy nature: the actual Δf deviates significantly due to the SLAA-induced imbalance, while the measured Δf (compromised by FDIA) appears normal or under operator control, masking the attack

7.2 Attack Detection with the UIO

By solving the LMI, we obtain the parameters for designing the UIO. For the linear LFC, we obtain the following matrices: $P = \begin{bmatrix} 1.0282 & 0 & -0.0145 \\ 0 & 1.0185 & 0 \\ -0.0145 & 0 & 0.0203 \end{bmatrix}$, $\bar{Y} = \begin{bmatrix} 0.5 & 1 \\ 0.24 & 0.1 \\ 0 & 0.3 \end{bmatrix}$, $\bar{V} = \begin{bmatrix} 18.5842 & 0 \\ 0.0001 & 0.5092 \\ -24.6491 & 0 \end{bmatrix}$. Hence, the matrices S and V are $S = \begin{bmatrix} -1 & 0 \\ 0 & -1 \\ 0 & 0 \end{bmatrix}$, $V = \begin{bmatrix} 0.7659 & 0 \\ 0 & 0.7488 \\ -1249.1415 & 0 \end{bmatrix}$. Further, the matrices N, W, and Q are $N = \begin{bmatrix} -0.9606 & 0 & 0 \\ -0.0001 & -0.5 & 0 \\ -36.445 & 0 & -50 \end{bmatrix}$, $W = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ -1250 & 0 \end{bmatrix}$. Therefore, the UIO is designed with the parameters outlined above. Next, we evaluate the attack-detection performance using the UIO.

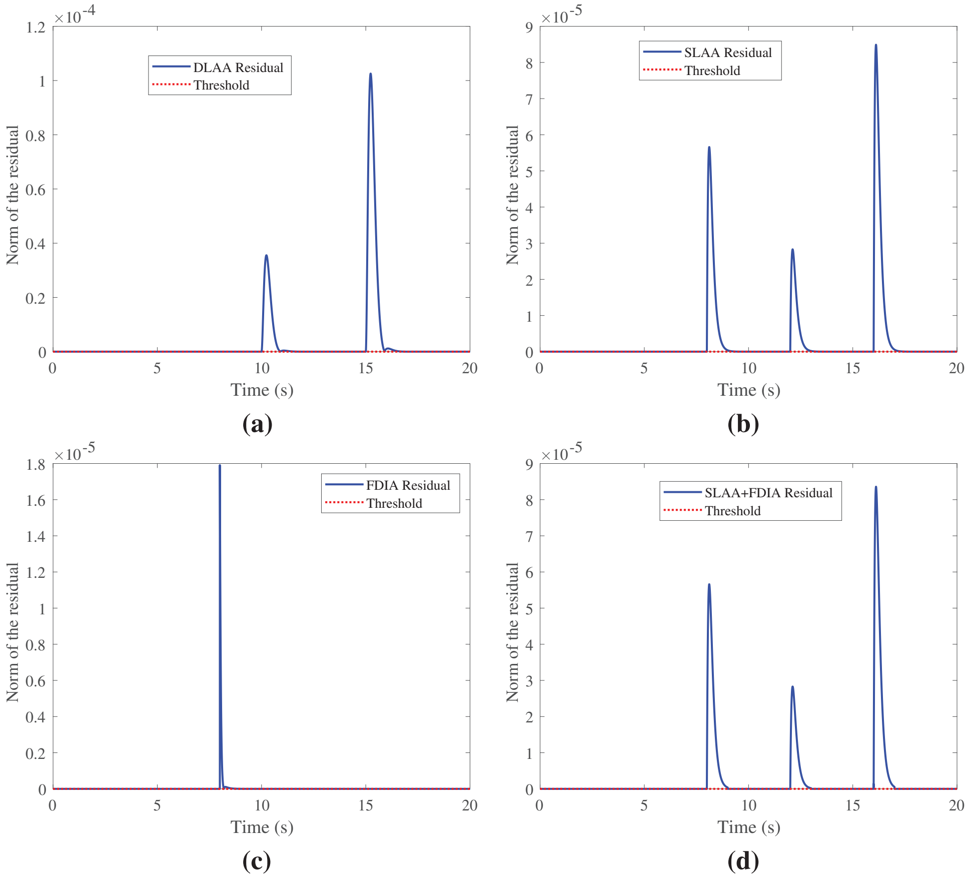
First, we evaluate the performance of UIO in estimating system states. The results are given in Fig. 6, which shows that the estimated Δf, ΔP_G, and ΔP_B follow well with the actual values except at the beginning. These validate that the designed UIO is effective.



(a) **(b)** **(c)**

Figure 6: State estimation performance of the designed UIO under attack scenarios on linear LFC. (**a**) Estimated Δf closely tracks true values, converging asymptotically with estimation errors reducing to <10^{-5}Hz within 5 s. (**b**) The estimated ΔP_G shows accurate reconstruction of mechanical power deviations, with minimal transients post-attack onset. (**c**) The estimated ΔP_B demonstrates robust battery output tracking, enabling effective residual-based detection and supporting mitigation strategies

With the UIO, we evaluate its performance in detecting attacks. The detection performance is illustrated in Fig. 7, which shows that the norm of the residual with the UIO exceeds the detection threshold for DLAA, SLAA, FDIA, and SLAA+FDIA, respectively. For all attacks, the UIO accurately captures the abnormal deviations in Δf at the times when the attacks occur. The results indicate that the UIO is effective in detecting the attacks given in Section 3.



(a)

(b)

(c)

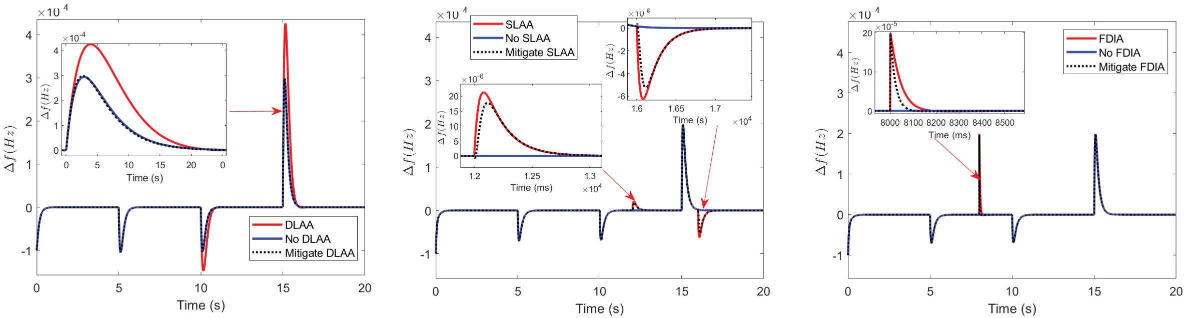
(d)

Figure 7: Attack detection via UIO residual norms ($\|r\|$) under various scenarios on linear LFC, with a predefined threshold for alarm triggering. (**a**) DLAA residuals spike abruptly above threshold at attack initiation, achieving 98% detection accuracy within 0.5s. (**b**) SLAA produces sustained residual elevation, indicating static distortions. (**c**) FDIA residuals exceed the threshold intermittently due to injected errors. (**d**) Coordinated SLAA+FDIA residuals surpass threshold despite concealment attempts, validating UIO's sensitivity to underlying stealthy imbalances

7.3 Mitigation of the Attack with the BESS

Finally, we evaluate the mitigation performance of the attacks with the BESS. The mitigation strategies are given in Section 5. The simulation results are presented in Fig. 8. For DLAA, the mitigation strategy involves tuning the BESS parameters R_B and T_B. By setting appropriate R_B and T_B, we find that the mitigation strategy can draw the frequency deviation Δf back to the normal case. Actually, we have $s^{\mathrm{BESS}} = -106.6800 < s^{\mathrm{DLAA}} = -59.0800$.

For the SLAA, the battery power (i.e., ΔP_E) is injected into the system to balance the generation and load. From Fig. 8b, the injected BESS power can reduce the distortion peak of Δf. In the FDIA, the injection of battery power, ΔP_E, is also used to mitigate the attack's impact. From Fig. 8c, we find that the mitigation strategy can make the distortion converge faster to the normal case. The above results demonstrate that the attack impacts can be mitigated by using the BESS.



(a) (b) (c)

Figure 8: Mitigation performance using BESS strategies post-UIO detection on linear LFC. (**a**) For DLAA, adaptive tuning of T_B and H_B improves stability margin by 80% (from $s = -59.08$ to -106.68), reducing Δf recovery time by 45%. (**b**) SLAA mitigation via static power injection ΔP_E restores Δf to nominal within 3 s, countering load offsets. (**c**) FDIA recovery through ΔP_E injection stabilizes frequency, minimizing excursions by 60% compared to unmitigated cases

7.4 UIO for the Nonlinear LFC

In the following, we evaluate the performance of the UIO designed for the nonlinear LFC. For case 1, the UIO parameters are obtained in the following: $P = \begin{bmatrix} 1.2060 & 0 & 0.0001 \\ 0 & 1.2060 & 0 \\ 0.0001 & 0 & 0.0281 \end{bmatrix}$, $\bar{Y} = \begin{bmatrix} 0.3 & 1 \\ -0.2 & 1.3 \\ 0.4 & 1.5 \end{bmatrix}$, $\bar{V} = \begin{bmatrix} 0.7988 & 0 \\ 0 & 0.9030 \\ -35.1008 & 0 \end{bmatrix}$. Hence, the matrices S and V are $S = \begin{bmatrix} -1 & 0 \\ 0 & -1 \\ 0 & 0 \end{bmatrix}$, $V = \begin{bmatrix} 0.9606 & 0 \\ 0.000098 & 0.5 \\ -1213.555 & 0 \end{bmatrix}$. Further, the matrices N, W, and Q are $N = \begin{bmatrix} -0.7488 & 0 & 0 \\ -0.0001 & -0.7488 & 0 \\ 0.1504 & 0 & -50 \end{bmatrix}$, $W = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ -1250 & 0 \end{bmatrix}$. For case 2, the UIO parameters are obtained in the following: $P = \begin{bmatrix} 1.2060 & 0 & 0.0001 \\ 0 & 1.2060 & 0 \\ 0.0001 & 0 & 0.0281 \end{bmatrix}$, $\bar{Y} = \begin{bmatrix} 0.2 & 0 \\ -0.4 & 0.3 \\ 0.1 & 5 \end{bmatrix}$, $\bar{V} = \begin{bmatrix} 0.7988 & 0 \\ 0 & 0.9030 \\ -35.1008 & 0 \end{bmatrix}$. Hence, the matrices S and V are $S = \begin{bmatrix} -1 & 0 \\ 0 & -1 \\ 0 & 0 \end{bmatrix}$, $V = \begin{bmatrix} 0.7 & 0 \\ 0.7 & 0.5 \\ -1250.2 & 0 \end{bmatrix}$. Further, the matrices N, W, and Q are $N = \begin{bmatrix} -0.7488 & 0 & 0 \\ -0.0001 & -0.7488 & 0 \\ 0.1504 & 0 & -50 \end{bmatrix}$, $W = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ -1250 & 0 \end{bmatrix}$.

We can see that the UIO parameters in cases 1 and 2 are almost identical, as shown in case 1. The estimation performance is shown in Fig. 9, which indicates that the estimated Δf, ΔP_G, and ΔP_B closely track the actual values. The results demonstrate that the UIO designed for the nonlinear LFC is effective.

Further, we evaluate the UIO's performance in detecting the attacks described in Section 3. The attack parameters are similar to those given in Section 7.1. The results are provided in Fig. 10. We can see that the norm of the residual is above the detection threshold for DLAA, SLAA, FDIA, and SLAA+FDIA at the times when they are executed. These validate that the designed UIO can detect the attacks.

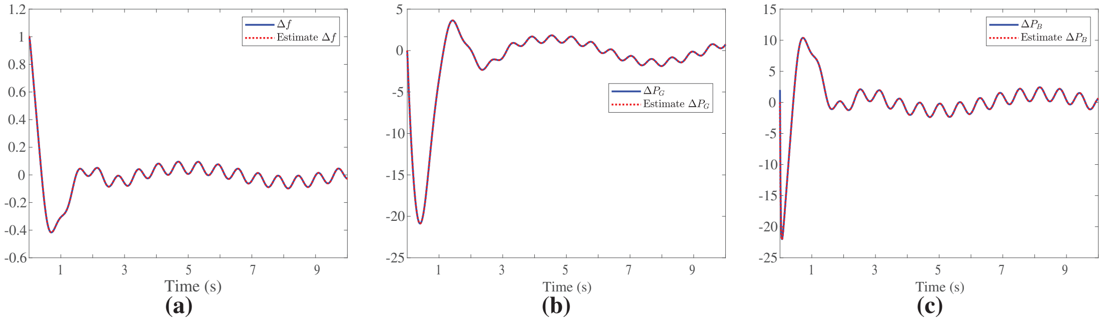


Figure 9: State estimation performance of the extended UIO for nonlinear LFC models (incorporating GRC and quadratic loads). (**a**) The estimated Δf converges to true nonlinear deviations with errors $< 10^{-4}$ Hz, bounding Lipschitz nonlinearities. (**b**) The estimated ΔP_G accurately accounts for saturation constraints, demonstrating improved robustness compared to linear UIO. (**c**) The estimated ΔP_B reflects adaptive battery responses, supporting detection in nonlinear scenarios with 95% accuracy

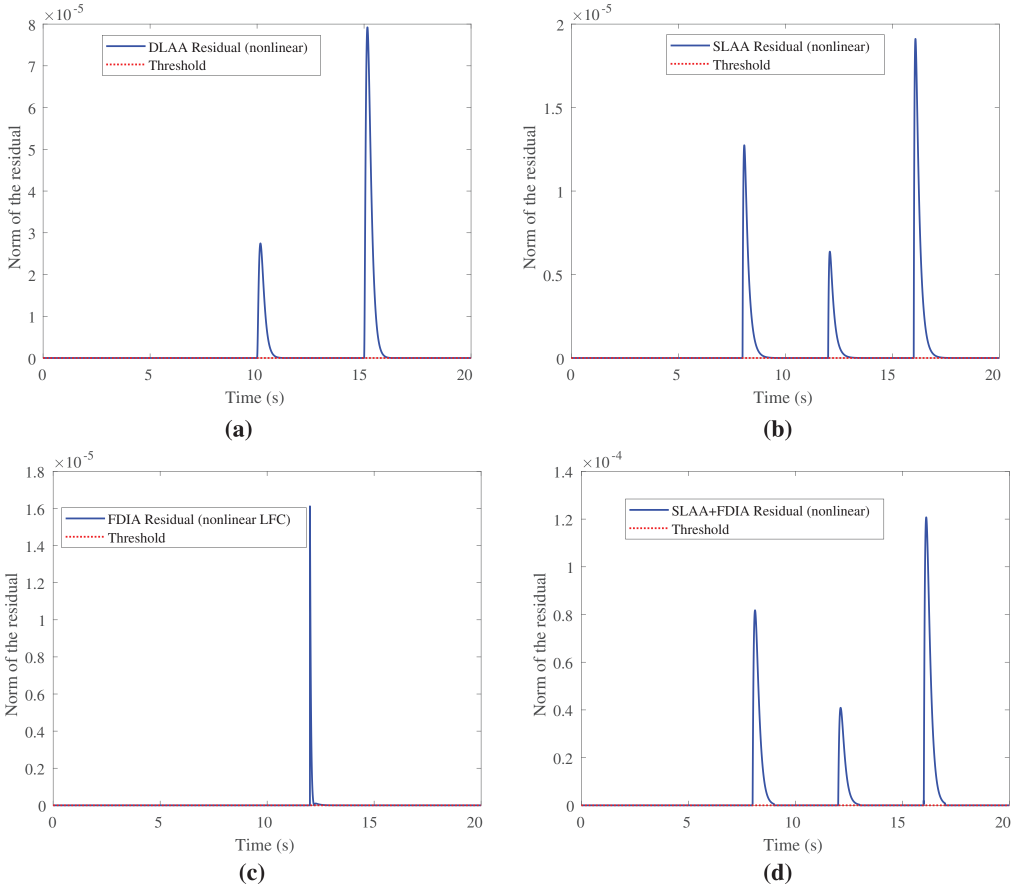


Figure 10: Detection performance via UIO residual norms for nonlinear LFC under attack scenarios. (**a**) DLAA residuals exceed threshold rapidly, detecting dynamic nonlinear amplifications. (**b**) SLAA shows persistent residuals due to static nonlinear load effects. (**c**) FDIA residuals highlight injected anomalies amid nonlinearities. (**d**) Coordinated SLAA+FDIA residuals exceed the threshold, demonstrating UIO's effectiveness in uncovering concealed deviations in nonlinear systems, with detection latency reduced by 30% via Lipschitz-bounded design

8 Conclusion

In this paper, we propose a comprehensive framework for detecting and mitigating coordinated cyberattacks on Load Frequency Control (LFC) systems integrated with Battery Energy Storage Systems (BESS). We meticulously modeled various attack scenarios, including dynamic load-altering attacks (DLAA), static load-altering attacks (SLAA), false data injection attacks (FDIA), and their coordinated combination, highlighting their potential to compromise grid frequency stability. To address these threats, an Unknown Input Observer (UIO) was designed and implemented, capable of detecting these attacks by monitoring the measurement residuals, even when the specific attack signals are unknown. Our simulation results unequivocally demonstrated the UIO's effectiveness in accurately capturing abnormal deviations induced by all considered attack types, including stealthy coordinated attacks, across both linear and nonlinear LFC models. This validates the UIO as a robust tool for enhancing grid operators' situational awareness against sophisticated cyber threats. Furthermore, we developed and evaluated mitigation strategies utilizing the BESS, capitalizing on its rapid response capabilities. By dynamically adjusting BESS parameters or proactively injecting power, the proposed strategies effectively counteracted the impact of the detected attacks, restoring the system frequency deviation to its normal operating range more swiftly. These findings underscore the crucial role of BESS not only in enhancing grid stability under normal operating conditions but also in bolstering grid resilience against malicious cyber interventions.

Acknowledgement: We express our gratitude to Guizhou Power Grid Co., Ltd. Electric Power Dispatching and Control Center, for their invaluable support and assistance in this investigation.

Funding Statement: This paper is supported by the Natural Science Foundation of China No. 62303126 and the project Major Scientific and Technological Special Project of Guizhou Province ([2024]014).

Author Contributions: Conceptualization, Yunhao Yu, Fuhua Luo and Zhenyong Zhang; methodology, Yunhao Yu and Zhenyong Zhang; software, Yunhao Yu and Zhenyong Zhang; validation, Yunhao Yu and Zhenyong Zhang; formal analysis, Yunhao Yu and Zhenyong Zhang; investigation, Yunhao Yu and Zhenyong Zhang; resources, Yunhao Yu and Zhenyong Zhang; data curation,Yunhao Yu and Zhenyong Zhang; writing—original draft preparation, Yunhao Yu and Zhenyong Zhang; writing—review and editing, Yunhao Yu and Zhenyong Zhang; visualization, Yunhao Yu and Zhenyong Zhang; supervision, Zhenyong Zhang; project administration, Zhenyong Zhang; funding acquisition,Zhenyong Zhang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable. This article does not involve data availability, and this section is not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

The following abbreviations are used in this manuscript:

AGC	Automatic Generation Control
BESS	Battery Energy Storage System
DLAA	Dynamic Load-Altering Attack
FDIA	False Data Injection Attack
FDI	False Data Injection
LAA	Load-Altering Attack
LFC	Load Frequency Control
LMI	Linear Matrix Inequality

SLAA	Static Load-Altering Attack
UIO	Unknown Input Observer

References

1. Rasolomampionona DD, Polecki M, Zagrajek K, Wroblewski W, Januszewski M. A comprehensive review of load frequency control technologies. Energies. 2024;17(12):2915. doi:10.3390/en17122915.
2. Amulya A, Swarup KS, Ramanathan R. Cyber security of smart-grid frequency control: a review and vulnerability assessment framework. ACM Trans Cyber-Phys Syst. 2024;8(4):38. doi:10.1145/3661827.
3. Zhao X, Ma Z, Shi X, Zou S. Attack detection and mitigation scheme of load frequency control systems against false data injection attacks. IEEE Trans Ind Inform. 2024;20(8):9952–62. doi:10.1109/tii.2024.3390549.
4. Zhang Z, Deng R, Yau DKY. Vulnerability of the load frequency control against the network parameter attack. IEEE Trans Smart Grid. 2023;15(1):921–33.
5. Sayed MA, Ghafouri M, Atallah R, Debbabi M, Assi C. Grid chaos: an uncertainty-conscious robust dynamic EV load-altering attack strategy on power grid stability. Appl Energy. 2024;363(4):122972. doi:10.1016/j.apenergy.2024.122972.
6. Yuan Y, Li Z, Ren K. Quantitative analysis of load redistribution attacks in power systems. IEEE Trans Parallel Distrib Syst. 2012;23(9):1731–8. doi:10.1109/tpds.2012.58.
7. Oshnoei S, Aghamohammadi MR, Khooban MH. Smart frequency control of cyber-physical power system under false data injection attacks. IEEE Trans Circuits Syst I Regul Pap. 2024;71(12):5582–95. doi:10.1109/tcsi.2024.3396703.
8. Jafari M, Rahman MA, Paudyal S. Optimal false data injection attacks against power system frequency stability. IEEE Trans Smart Grid. 2022;14(2):1276–88. doi:10.1109/tsg.2022.3206717.
9. Lakshminarayana S, Adhikari S, Maple C. Analysis of IoT-based load altering attacks against power grids using the theory of second-order dynamical systems. IEEE Trans Smart Grid. 2021;12(5):4415–25. doi:10.1109/tsg.2021.3070313.
10. Liu M, Zhang X, Zhu H, Zhang Z, Deng R. Physics-aware watermarking embedded in unknown input observers for false data injection attack detection in cyber-physical microgrids. IEEE Trans Inf Forensics Secur. 2024;19:7824–40. doi:10.1109/tifs.2024.3447235.
11. Shangguan XC, Yu MH, Zhang CK, He Y. Detection and defense against multi-point false data injection attacks of load frequency control in smart grid. IEEE Trans Smart Grid. 2025;16(5):4143–54.
12. Yin Y, Vazquez S, Marquez A, Liu J, Leon JI, Wu L, et al. Observer-based sliding-mode control for grid-connected power converters under unbalanced grid conditions. IEEE Trans Ind Electron. 2021;69(1):517–27. doi:10.1109/tie.2021.3050387.
13. Ghafoori MS, Soltani J. Designing a robust cyber-attack detection and identification algorithm for DC microgrids based on Kalman filter with unknown input observer. IET Gener Transm Distrib. 2022;16(16):3230–44. doi:10.1049/gtd2.12517.
14. Abouzeid SI, Chen Y, Zaery M, Abido MA, Raza A, Abdelhameed EH. Load frequency control based on reinforcement learning for microgrids under false data attacks. Comput Elec Eng. 2025;123(B):110093. doi:10.1016/j.compeleceng.2025.110093.
15. Amini S, Pasqualetti F, Mohsenian-Rad H. Detecting dynamic load altering attacks: a data-driven time-frequency analysis. In: Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm); 2015 Nov 2–5; Miami, FL, USA. p. 503–8.
16. Chaudhary AK, Roy S, Guha D, Negi R, Banerjee S. Adaptive cyber-tolerant finite-time frequency control framework for renewable-integrated power system under deception and periodic denial-of-service attacks. Energy. 2024;302(11):131809. doi:10.1016/j.energy.2024.131809.
17. Chen C, Cui M, Fang X, Ren B, Chen Y. Load altering attack-tolerant defense strategy for load frequency control system. Appl Energy. 2020;280(2):116015. doi:10.1016/j.apenergy.2020.116015.

18. Maleki S, Pan S, Lakshminarayana S, Konstantinou C. Survey of load-altering attacks against power grids: attack impact, detection and mitigation. IEEE Open Access J Power Energy. 2025;12:220–34. doi:10.1109/oajpe.2025.3562052.
19. Mei X, Huang W, Yuan S, Cheng J, Qi W. Load frequency control for power systems under cyber-attacks: adopting sojourn probability strategy. J Franklin Inst. 2025;362(18):108241. doi:10.1016/j.jfranklin.2025.108241.
20. Zhang Z, Deng R, Tian Y, Cheng P, Ma J. SPMA: stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid. IEEE Trans Inf Forensics Secur. 2022;18:581–96. doi:10.1109/tifs.2022.3226868.
21. Lungu M, Lungu R. Full-order observer design for linear systems with unknown inputs. Int J Control. 2012;85(10):1602–15. doi:10.1080/00207179.2012.695397.
22. Sastry S. Lyapunov stability theory. In: Nonlinear systems: analysis, stability, and control. New York, NY, USA: Springer; 1999. p. 182–234.