

Critical Boundary Index-based Preventive and Post-detection Defense Approach Against False Data Injection Attacks in Power Systems with Distributed Energy Resources

Masahiro Furukakoi, *Member, IEEE*, Akito Nakadomari, *Member, IEEE*, Akie Uehara, *Member, IEEE*, Paras Mandal, *Senior Member, IEEE*, Mitsunaga Kinjo, *Member, IEEE*, and Tomonobu Senjyu, *Fellow, IEEE*

Abstract—Cybersecurity in power systems with distributed energy resources (DERs) has become a serious challenge. This paper proposes a critical boundary index (CBI)-based preventive and post-detection defense approach against false data injection attacks (FDIAs) in power systems with DERs. The proposed approach utilizes the inherent attack resistance of CBI, a voltage stability index previously developed by the authors, to both preventively limit the impact of attacks and provide high-sensitivity post-attack detection of data manipulation. This paper quantitatively evaluates voltage stability monitoring approaches against FDIAs, comparing the resilience of CBI with conventional indices. Verification is conducted using IEEE 5-bus and 118-bus test systems with two types of FDIA scenarios: detection-avoidance type and misdirection type. The results demonstrate that when CBI is employed for monitoring, the achievable false data injection by attackers aiming to cause voltage drops is significantly reduced compared with conventional indices, maintaining system voltage within stable ranges. Additionally, CBI shows 1.5–2 times higher detection sensitivity compared with conventional indices. Notably, CBI demonstrates effective detection capability even against sophisticated attacks that falsely show improvement in voltage stability indices, which are difficult to detect using conventional approaches. These results confirm that the proposed approach effectively constrains attacker capabilities while providing enhanced detection sensitivity. Based on these findings, the proposed approach is shown to provide high sensitivity to even minor data tampering, offering a multi-layered defense combining prevention and detection for power systems with DERs.

Index Terms—Critical boundary index (CBI), cybersecurity, distributed energy resource (DER), false data injection attack (FDIA), voltage stability.

Manuscript received: October 8, 2025; revised: January 21, 2026; accepted: March 26, 2026. Date of CrossCheck: March 26, 2026. Date of online publication: June 8, 2026.

This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>).

M. Furukakoi (corresponding author) is with Sanyo-Onoda City University, Yamaguchi 756-0884, Japan (e-mail: furukakoi@rs.socu.ac.jp).

A. Nakadomari is with Saitama University, Saitama 338-8570, Japan (e-mail: nakadomari@mail.saitama-u.ac.jp).

A. Uehara, M. Kinjo, and T. Senjyu are with University of the Ryukyus, Okinawa 903-0213, Japan (e-mail: uehara_a@cs.u-ryukyu.ac.jp; mitsu18@tec.u-ryukyu.ac.jp; b985542@tec.u-ryukyu.ac.jp).

P. Mandal is with The University of Texas at El Paso, El Paso, USA (e-mail: pmandal@utep.edu).

DOI: 10.35833/MPCE.2025.000962

I. INTRODUCTION

POWER systems are essential infrastructures of modern society, and ensuring their stable operation is of paramount importance. In recent years, with the advancement of power system digitalization, the threat of cyberattacks has become increasingly evident worldwide. The vulnerability of supervisory control and data acquisition (SCADA) systems to cyberattacks has been recognized for over a decade [1], with early frameworks establishing the importance of systematic vulnerability assessment at multiple levels. As power systems have evolved, comprehensive surveys [2] have documented how the integration of computing and communication capabilities introduces numerous vulnerabilities to the cyber-physical system. The large-scale power outage in Ukraine in 2015, which affected approximately 0.23 million people, is a representative case where remote control systems of substations were targeted [2], [3]. Additionally, in 2021, oil pipelines in the United States were subjected to ransomware attacks, leading to significant disruption to fuel supply [4]. These cases show that cyberattacks on energy infrastructure are becoming increasingly serious.

In this context, with the expansion of renewable energy, the adoption of distributed energy resources (DERs) is rapidly progressing. Compared with conventional centralized power sources, DERs are geographically distributed control points and, in many cases, remotely monitored and controlled via the internet. This characteristic creates new vulnerabilities from a cybersecurity perspective [5]. Research examining inverter-based microgrids [6] and distribution grids with high DER penetration [7] has illustrated how various cyberattacks affect system resilience and what mitigation strategies might be effective. In Japan, for instance, unauthorized access to remote monitoring systems of solar power generation facilities was confirmed in 2022, highlighting the risk of data tampering and issuance of control commands [8]. Similarly, in 2022, an attack targeting vulnerabilities in monitoring control systems at wind power generation facilities in Europe resulted in temporary suspension of output control functions at multiple power plants [9].

The importance of monitoring and evaluating power sys-



tem stability is increasing under these circumstances. In particular, voltage stability is one of the important indicators of system reliability, but it has been demonstrated that its evaluation can be distorted by false data injection attacks (FDIAs) on measurement data [10]. Research has shown that sophisticated attackers can bypass the conventional bad data detection (BDD), necessitating advanced anomaly detection algorithms [11]. An FDIA is a sophisticated cyberattack that strategically manipulates measurement values used for system state estimation, misleading the judgments of system operators. This paper compares the effectiveness of voltage stability monitoring methods against FDIAs in power systems with

DERs. Specifically, using IEEE standard test systems, we quantitatively evaluate the detection performances of conventional indices and the critical boundary index (CBI) [12].

Research on FDIA detection and countermeasures in power systems has developed rapidly in recent years. As shown in Table I, the research has been primarily conducted in three directions: ① construction of attack models, ② attack detection technologies, and ③ system defense approaches. These attack directions are interrelated, along with the development of new attack models that promote the evolution of attack detection technologies, which, in turn, leads to the proposal of more advanced system defense approaches.

TABLE I
COMPARISON OF RESEARCHES ON FDIA DETECTION AND COUNTERMEASURES IN POWER SYSTEMS

Reference	Year	Target	Approach	Countermeasure	Defense type
[13]	2025	AC state estimation	Stealthy attack using network uncertainty	Dynamic time warping (DTW) strategy and hierarchical clustering	Post-detection
[10]	2025	Voltage stability indices and DER voltage measurement data	Manipulation of voltage stability indices through bi-level optimization	Spatial-temporal anomaly detection using graph neural network (GNN)	Post-detection
[14]	2025	Power system measurement data, state estimation data	Residual detection bypass using Jacobian matrix	Detection using hypergraph model and subgraph partitioning	Post-detection
[15]	2025	Communication data between DERs	Communication link attack using bias injection	Detection-triggered mitigation and sensor strategy	Post-detection
[16]	2024	AC state estimation	Stealthy attack using artificial neural network (ANN) and BDD filtering	Measurement data protection using BDD	Preventive
[17]	2024	EV charging schedules	FDIA through bi-level optimization	Detection using machine learning (ML) and security-constrained unit commitment	Preventive and post-detection
[18]	2024	Price information in demand response (DR) systems	Smart meter attack using price manipulation	Zero-sum game and multi-agent reinforcement learning (MARL)	Post-detection
[19]	2023	Voltage control in distribution networks	Staged data manipulation	Improved voltage control mechanism and detection algorithm	Post-detection
[20]	2023	AC state estimation	Detection avoidance using latent space clustering	High-accuracy detection using self-supervised deep learning (SSDL)	Post-detection
[21]	2023	Data in integrated electricity-gas systems	Two-stage attack on gas-fired power plant fuel supply	High-risk measurement identification and ML detection	Preventive and post-detection
This paper		Active and reactive power (PQ) output data from DERs	Voltage stability index falsification and index improvement attacks	CBI-based preventive and post-detection defense utilizing inherent attack resistance of CBI [12]	Preventive and post-detection

1) Research on attack models

Reference [15] focuses on secondary FDIAs on communication links between DERs, evaluating the impact of various patterns of bias injection. Reference [13] proposes an attack model during the special situation of topology changes, analyzing techniques to enhance stealth by exploiting network uncertainties. In [21], the construction of a two-stage attack model targeting gas-fired power plants by utilizing the interdependence of power systems and gas networks is reported. The research indicates that attack models are becoming more sophisticated with the increasing complexity of systems.

2) Attack detection technologies

In the field of attack detection technology, machine learning and deep learning-based approaches have become prevalent. Reference [20] proposes a detection approach using self-supervised learning with stacked autoencoders (a type of neural network with multiple layers). Reference [10] develops a graph autoencoder-based detector against attacks on voltage stability-related data. Reference [14] proposes a detection approach combining subgraph partitioning strategies

and hypergraph models. While these approaches demonstrate high detection accuracy, they all assume detection after an attack has taken place.

3) System defense approaches

System defense approaches leveraging physical interconnections have attracted increasing attention. Reference [15] proposes an impact mitigation approach combining unknown input observers and power line-based physical verification. Reference [19] aims to strengthen the resilience from the design stage, deploying defense measures involving improved voltage control mechanisms and detection algorithms. Reference [16] proposes a completely blind detection approach that does not require topology knowledge.

As shown in Table I, most existing research adopts a “post-detection” approach, focusing on detecting and responding to attacks after they occur. In contrast, this paper is characterized by applying the CBI [12], which has inherent resistance to attacks, to realize a preventive and post-detection defense approach. The main contributions of this paper can be summarized as follows.

1) Proposal of a CBI-based preventive and post-detection defense approach. Unlike conventional post-detection-only approaches, the CBI-based one has inherent resistance to the attacks, enabling both preventive limitation of the impact of attacks and high-sensitivity post-attack detection of data manipulation.

2) Comparative evaluation of voltage stability monitoring approaches. We quantitatively compare the resilience of conventional indices and the CBI against FDIAs. Notably, while [10] does not compare the attack resilience of the indices themselves, this paper provides new insights in this regard.

3) Construction of practical attack scenarios. Two types of practical attack scenarios are designed, namely detection-avoidance type which maintains the voltage stability indices at pre-attack levels, and misdirection type which causes the voltage stability indices to falsely indicate improved stability. The latter represents a sophisticated camouflage attack that is difficult to detect with conventional approaches.

4) Response to minor data tampering. It is demonstrated that CBI, due to its characteristic of directly focusing on power flow changes, has high detection sensitivity to minor data tampering compared with conventional indices. This enables earlier detection of sophisticated attacks.

Through these contributions, this paper enhances the defense capabilities against sophisticated attacks such as FDIAs in modern power systems with DERs. The findings suggest the importance of multi-layer defense combining prevention and detection in power system security design, rather than relying on a single index or detection approach. The proposed approach is evaluated through quantitative simulations using IEEE standard test systems.

The remainder of this paper is organized as follows. Section II introduces the overview of FDIAs in power systems and describes the attack scenario design. Section III presents the voltage stability monitoring approaches, including conventional indices and the CBI in this paper. Section IV details the case studies and presents simulation results for both IEEE 5-bus and IEEE 118-bus test systems. Finally, Section V concludes this paper and presents future research directions.

II. OVERVIEW OF FDIAs IN POWER SYSTEMS AND ATTACK SCENARIO DESIGN

A. Overview of FDIAs in Power Systems

FDIAs in power systems involve deliberately manipulating measurement data used for state monitoring, misleading the judgment of system operators. In particular, the manipulation of PQ data directly affects voltage stability evaluation and may cause serious incidents in power systems.

A key characteristic of FDIAs is the sophisticated manipulation of data to satisfy the physical constraints of power systems. This makes the detection using conventional approaches difficult. As illustrated in Fig. 1, when an attacker tampers with PQ data at the measurement points, the resulting state estimation may lead system operators to incorrectly perceive a drop in bus voltages, even though no actual anomaly

is present. Consequently, operators might implement unnecessary emergency controls such as load shedding. Such attacks not only compromise the reliability of power supply, but can also cause economic losses and social disruption. Note that in Fig. 1, P_{false} and Q_{false} are the falsified active and reactive power, respectively.

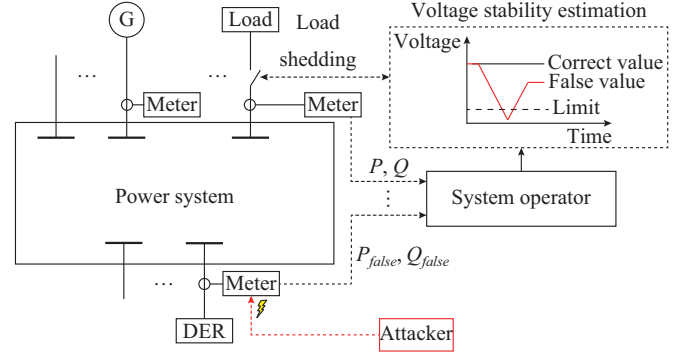


Fig. 1. Conceptual framework of FDIA mechanism leading to unnecessary load shedding.

In modern power systems with DERs, the increase in monitoring and control points and the expansion of communication networks have multiplied potential attack entry points. Furthermore, in an operational environment that prioritizes real-time response, the time available for detailed analysis to detect attacks is limited, thereby necessitating more effective defense approaches.

B. Attack Scenario Design

In this paper, we consider two types of practical attack scenarios, as classified in Table II. Scenario A is a detection-avoidance type that maintains voltage stability indices at pre-attack levels to evade detection of data manipulation. In this scenario, the index values remain unchanged, making the system state appear normal and thus making attack detection difficult. Conversely, Scenario B is a misdirection type designed to make voltage stability indices appear improved, misleading system operators into believing that the system is more stable than it actually is. This is a more sophisticated camouflage attack that reduces operator vigilance, potentially delaying necessary countermeasures for a deteriorating system state.

TABLE II
CLASSIFICATION OF PRACTICAL ATTACK SCENARIOS

Scenario	Description
A	An FDIA is designed to maintain voltage stability indices at pre-attack levels, masking the presence of malicious data manipulation
B	An FDIA is crafted to exhibit artificial improvements in voltage stability indices, potentially misleading system operators about stability state

Let $\mathcal{A} \subset \mathcal{B}$, where $\mathcal{A}$ denotes the set of attacked buses; and $\mathcal{B}$ denotes the set of all buses. The attacker determines the amount of PQ data manipulation by solving the optimization problem (1).

$$\min_{\Delta P_{\text{attack}}, \Delta Q_{\text{attack}}} \min_{i \in \mathcal{B}} V_i \quad (1)$$

where V_i is the voltage magnitude at bus i ; and ΔP_{attack} and ΔQ_{attack} are the vectors of false active and reactive power injected at the attacked buses, with their per-bus components $P_{\text{attack},i}$ and $Q_{\text{attack},i}$ respectively.

Problem (1) is subject to the following constraints.

For attacked bus $i \in \mathcal{A}$, we have:

$$P_{\text{false},i} = P_{\text{true},i} + \Delta P_{\text{attack},i} \quad \forall i \in \mathcal{A} \quad (2)$$

$$Q_{\text{false},i} = Q_{\text{true},i} + \Delta Q_{\text{attack},i} \quad \forall i \in \mathcal{A} \quad (3)$$

where $P_{\text{true},i}$ and $Q_{\text{true},i}$ are the actual active and reactive power measurements on bus i , respectively; $\Delta P_{\text{attack},i}$ and $\Delta Q_{\text{attack},i}$ are the amounts of false PQ data injected by the attacker on bus i , respectively; and $P_{\text{false},i}$ and $Q_{\text{false},i}$ are the falsified active and reactive power values on bus i , respectively.

The power injection at each bus is defined as:

$$P_i = \begin{cases} P_{\text{false},i} & i \in \mathcal{A} \\ P_{\text{true},i} & i \in \mathcal{B} \setminus \mathcal{A} \end{cases} \quad (4)$$

$$Q_i = \begin{cases} Q_{\text{false},i} & i \in \mathcal{A} \\ Q_{\text{true},i} & i \in \mathcal{B} \setminus \mathcal{A} \end{cases} \quad (5)$$

where P_i and Q_i are the active and reactive power injections used in state estimation, respectively, which are falsified values for attacked buses and true values for non-attacked buses. These power injections must satisfy the power flow equations as:

$$P_i = V_i \sum_{j \in \mathcal{B}} V_j (G_{ij} \cos \delta_{ij} + B_{ij} \sin \delta_{ij}) \quad \forall i \in \mathcal{B} \quad (6)$$

$$Q_i = V_i \sum_{j \in \mathcal{B}} V_j (G_{ij} \sin \delta_{ij} - B_{ij} \cos \delta_{ij}) \quad \forall i \in \mathcal{B} \quad (7)$$

where G_{ij} and B_{ij} are the real and imaginary parts of element (i,j) of the bus admittance matrix $\mathbf{Y}$, respectively; and $\delta_{ij} = \delta_i - \delta_j$ is the voltage angle difference between buses i and j , and δ_i and δ_j are the voltage angles of buses i and j , respectively.

The power flow equations (6) and (7) with power injections defined in (4) and (5) ensure that the physical relationships in the power system are preserved, allowing the false data to bypass conventional BDD mechanisms of state estimators. In typical power flow calculations, the system operator specifies active and reactive power at PQ buses (such as DER connection points), while the power flow equations determine the resulting voltages and power flows. When attackers falsify the active and reactive values at PQ buses, the power flow calculation converges normally using these falsified values, and the system operator cannot detect the manipulation because the calculated results satisfy all physical constraints. The attack is designed such that while voltage stability indices appear normal, the actual bus voltages calculated from the falsified data become lower than they should be (objective function (1)). In addition to these power balance constraints, the optimization problem is subject to standard operational constraints including voltage limits and line flow limits.

In Scenario A, the following constraint is added:

$$|VSI(P_{\text{false}}, Q_{\text{false}}) - VSI(P_{\text{true}}, Q_{\text{true}})| \leq \epsilon \quad (8)$$

where VSI is the value of any voltage stability index; and ϵ is the tolerance error. This constraint keeps the difference between pre- and post-attack voltage stability indices small, making it difficult to detect attacks through index monitoring. For CBI, the same constraint applies:

$$|CBI(P_{\text{false}}, Q_{\text{false}}) - CBI(P_{\text{true}}, Q_{\text{true}})| \leq \epsilon \quad (9)$$

where CBI is the value of the CBI.

In Scenario B, the following constraint is added:

$$VSI(P_{\text{false}}, Q_{\text{false}}) < VSI(P_{\text{true}}, Q_{\text{true}}) \quad (10)$$

Note that the direction of the inequality in (10) corresponds to conventional indices, namely the fast voltage stability index (FVSI), line stability index (L_{mn}), active power stability index (L_p), and novel line stability index (NLSI), all of which indicate a less stable condition as their values approach 1. Therefore, disguising an apparent improvement requires making the post-attack value smaller. Conversely, as shown in Table III, CBI is zero at the voltage collapse point, with larger values indicating more stable conditions. Therefore, for CBI, the inequality in (10) is reversed as:

$$CBI(P_{\text{false}}, Q_{\text{false}}) > CBI(P_{\text{true}}, Q_{\text{true}}) \quad (11)$$

TABLE III
STABILITY RANGES AND VOLTAGE COLLAPSE POINTS OF DIFFERENT
VOLTAGE STABILITY INDICES

Index	Stability range	Voltage collapse point
FVSI [22]	[0, 1]	1
L_{mn} [23]	[0, 1]	1
L_p [24]	[0, 1]	1
NLSI [25]	[0, 1]	1
CBI [12]	[0, +∞)	0

The inequality (11) ensures that CBI appears to increase after the attack, falsely indicating improved system stability. In either case, the essential attack intention remains the same, i.e., making the system state appear improved.

By solving this optimization problem, the attacker can determine the optimal amount of data manipulation to cause the intended voltage drop while satisfying the physical constraints of the system. These attack scenarios simulate realistic threats and are suitable for evaluating the resilience of voltage stability monitoring approaches.

III. VOLTAGE STABILITY MONITORING APPROACHES

A. Conventional Indices

Various indices have been proposed to evaluate voltage stability in power systems. Figure 2 shows the two-bus system model for voltage stability analysis with transmission parameters, from which various voltage stability indices are derived, where a transmission line with impedance $Z \angle \theta = r_{ik} + jx_{ik}$ connects buses i and k with a phase angle difference of $\delta = \delta_i - \delta_k$ between them; Z is the transmission line impedance; θ is the transmission line impedance angle; P_k and Q_k are the receiving-end active power and reactive power, respectively; and x_{ik} and r_{ik} are the transmission line reactance

and resistance, respectively. The power flow equations for this system form the basis for developing various voltage stability indices.

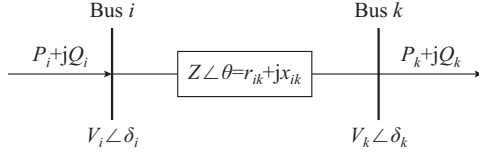


Fig. 2. Two-bus system model for voltage stability analysis with transmission parameters.

As shown in Table III, representative indices include FVSI, L_{mn} , L_p , NLSI. These indices are calculated from the voltage or power flow at both ends of transmission lines. Values approaching 1 indicate increasingly unstable voltage conditions.

The FVSI focuses on reactive power flow in transmission lines and is expressed by:

$$FVSI = \frac{4Z^2 Q_k}{V_i^2 x_{ik}} \quad (12)$$

where $FVSI$ is the value of the FVSI.

L_{mn} is an index considering the influence of phase angles and can be expressed as:

$$L_{mn} = \frac{4x_{ik} Q_k}{V_i^2 (\sin(\theta - \delta))^2} \quad (13)$$

L_p is an index focusing on active power flow angles and can be expressed as:

$$L_p = \frac{4r_{ik} P_k}{V_i^2 (\cos(\theta - \delta))^2} \quad (14)$$

NLSI is an index considering both active and reactive power and can be expressed as:

$$NLSI = \frac{4(P_k r_{ik} + Q_k x_{ik})}{V_i^2 (\cos \delta)^2} \quad (15)$$

where $NLSI$ is the value of the NLSI.

These conventional indices have demonstrated adequate effectiveness for evaluating voltage stability under steady-state conditions. However, their effectiveness against sophisticated attacks such as FDIAs has not been sufficiently verified. In particular, since these indices are all calculated based on the instantaneous state of transmission lines, there is a risk of producing erroneous stability evaluation if an attacker skillfully manipulates specific measurement values.

B. CBI

CBI was previously proposed as a VSI in [12]. As illustrated in Fig. 3, CBI represents the distance between the current operating point $K(P_k, Q_k)$ and the critical voltage stability boundary $C(X, Y)$ in the P - Q plane. The operating point K represents the active and reactive power flowing through the transmission line, while C describes the boundary beyond which the system becomes unstable and voltage collapse occurs.

CBI is calculated as:

$$CBI = \sqrt{\Delta P_{ik}^2 + \Delta Q_{ik}^2} \quad (16)$$

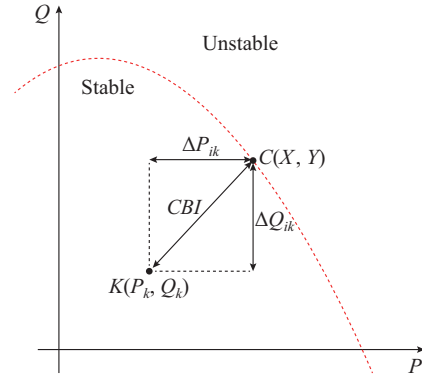


Fig. 3. Geometric interpretation of CBI in P - Q plane.

where ΔP_{ik} and ΔQ_{ik} are the P - and Q -components of the distance between the operating point and the critical boundary in the P - Q plane, respectively.

The characteristics of CBI are described as follows.

1) By directly focusing on power flow changes, CBI can detect the effects of data manipulation more sensitively compared with conventional indices. While conventional indices are calculated based on the steady state of transmission lines, CBI captures dynamic changes in power flow, potentially suitable for detecting even minor tampering.

2) By evaluating active and reactive power changes comprehensively, the detection of partial manipulation by attacks becomes possible. For example, even if an attacker only tampers with active power, the impact can be detected from changes in the power flow pattern of the overall system.

3) As shown in Table III, a larger CBI value indicates a more stable condition because it corresponds to a larger margin from the voltage collapse point, which facilitates intuitive understanding. Unlike conventional indices, whose values approach 1 as the system becomes less stable, CBI increases as the operating point moves further from voltage collapse.

The most distinctive feature of CBI is its focus on power flow changes rather than on the steady-state power flow conditions of transmission lines. This characteristic provides inherent resilience against attacks such as FDIAs that manipulate measurement values. Even if an attacker tampers with specific measurements, CBI can detect changes in the power flow pattern of the overall system, potentially mitigating the effect of attacks.

An important consideration in power systems with DERs is to distinguish between legitimate DER output variations and malicious FDIAs. DER output variations are typically constrained by grid codes such as ramp rate limits (e.g., 10% per min in many jurisdictions). Since CBI monitors power flow changes, sudden deviations exceeding these regulatory limits can serve as indicators of potential FDIAs rather than normal DER variability. Furthermore, DER output variations typically exhibit continuous, weather-correlated patterns, whereas FDIAs produce abrupt, discontinuous changes.

Furthermore, CBI is based on the physical behavior of the power system and is expected to have greater robustness

against data tampering compared with conventional indices that depend on data accuracy. In this paper, we quantitatively evaluate the detection performance of each index against FDIAs through the comparison between CBI and conventional indices.

IV. CASE STUDIES AND SIMULATION RESULTS

Figure 4 illustrates the evaluation framework to assess CBI resilience against FDIAs. The evaluation framework is divided into two phases: the attacker's process and the defender's process. In the attacker's process, bi-level optimization generates false data injection (ΔP_{attack} , ΔQ_{attack}) by minimizing bus voltages while satisfying power balance and scenario-specific constraints. The defender's process performs AC power flow calculations at PQ buses and calculates CBI values to detect attacks through two detection mechanisms corresponding to Scenarios A and B.

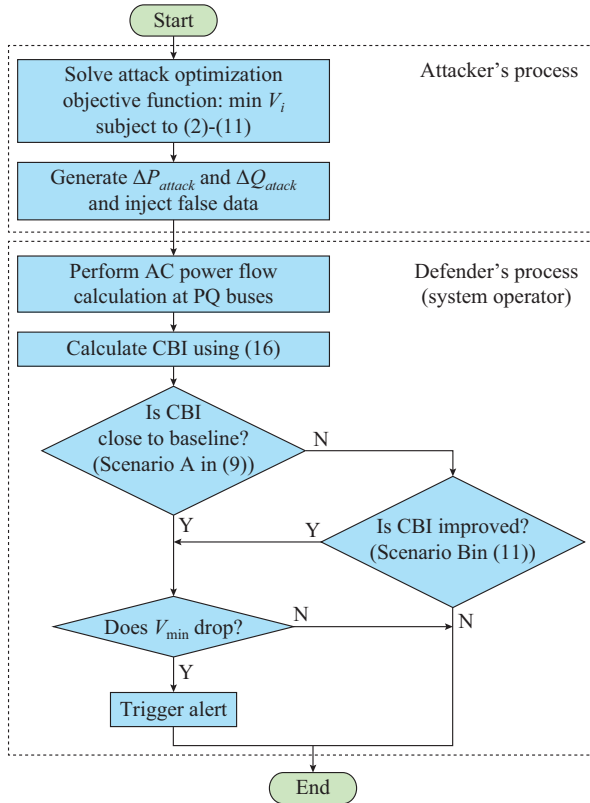


Fig. 4. Evaluation framework to assess CBI resilience against FDIAs.

A. Overview of Test Systems

In this paper, verification is conducted using IEEE 5-bus and 118-bus test systems. Modifications are made to each system to account for the integration of DERs and the presence of attackers. As shown in Fig. 5, the modified IEEE 5-bus test system consists of 7 transmission lines, 2 generators, and DERs, making it suitable for verifying basic system characteristics. DERs are installed at buses 3-5, and these measurement points are assumed to be attack targets. The parameters of each transmission line and bus are set as standard values from IEEE test systems [26].

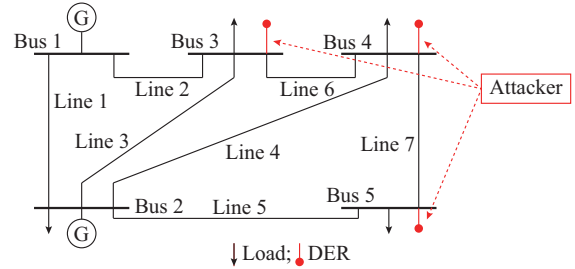


Fig. 5. Modified IEEE 5-bus test system.

Meanwhile, the modified 118-bus test system [27], as shown in Fig. 6, is a large-scale one with 179 transmission lines and multiple DERs, allowing verification under more practical conditions. In this large-scale system, simultaneous attack scenarios are considered on multiple buses located in different regions of the system such as buses 5, 15, 20, buses 50, 55, 60, and buses 85, 95, 105. This enables evaluation of the impact of attacks on different parts of the system on the overall stability.

Simulation is conducted using optimal power flow calculations at 1 s intervals, focusing on steady-state analysis without considering transient states. The attack optimization problem defined in Section II is solved using MATLAB Optimization Toolbox ("fmincon" function) for constrained nonlinear optimization. In both test systems, data tampering is simulated based on the attack scenarios defined in Section II. The simulation period is set to be 10 s, with FDIAs implemented at $t = 5$ s.

B. Verification in Modified IEEE 5-bus Test System

This subsection presents the verification results for the modified IEEE 5-bus test system in Scenarios A and B. To clarify the evaluation metrics, Figs. 7 and 8 show the temporal evolution of the minimum bus voltage (in per-unit) across the entire system in Scenarios A and B, respectively, which represents the actual physical state. In Figs. 7 and 8, the dotted line represents the correct (unattacked) voltage, and the solid lines represent voltages when different indices are used for system monitoring. In contrast, Figs. 9 and 10 compare the voltage stability indices for each transmission line before and after attacks in Scenarios A and B, respectively, which are used for system monitoring and attack detection. Understanding the relationship between these two metrics is essential for evaluating the effectiveness and deceptiveness of each attack scenario. Note that in Fig. 9, the left vertical axis shows the difference between pre-attack and post-attack index values (bar graph), and the right vertical axis shows the absolute index values (line graph with markers). In Figs. 9 and 10, "Before" and "After" denote pre-attack and post-attack values, respectively.

As shown in Fig. 7, conventional indices permit significant voltage degradation following the initiation of attack, with the L_p index allowing critical drops below 0.9 p.u.. In contrast, the proposed approach effectively constrains voltage reduction, maintaining the voltage levels above 0.95 p.u.. This demonstrates the inherent difficulty in causing substantial voltage degradation by the attackers when the proposed approach is employed.

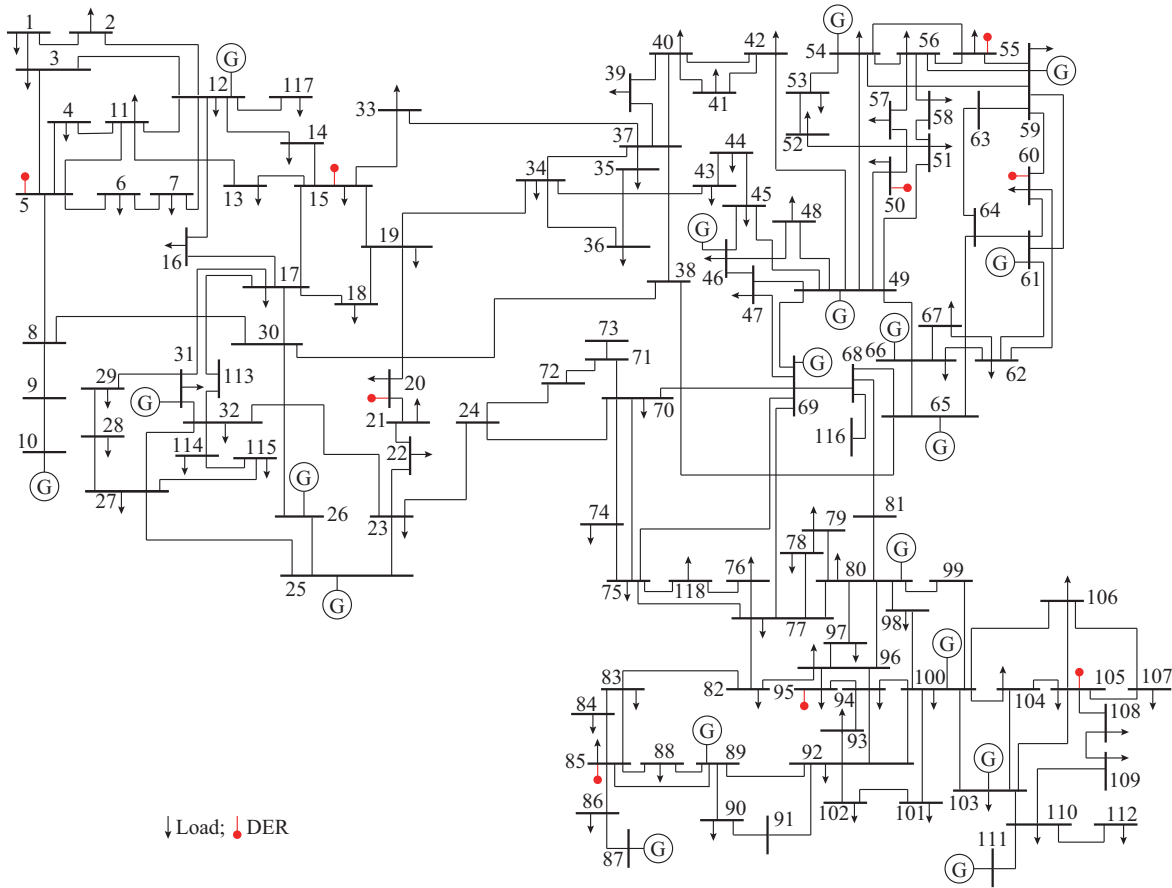


Fig. 6. Modified IEEE 118-bus test system.

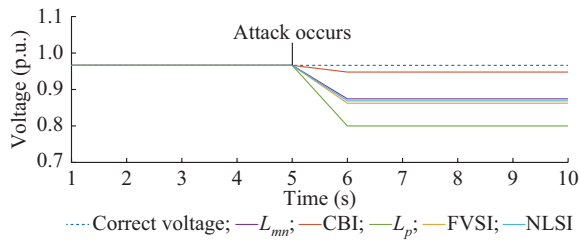


Fig. 7. Temporal evolution of the minimum bus voltage in Scenario A.

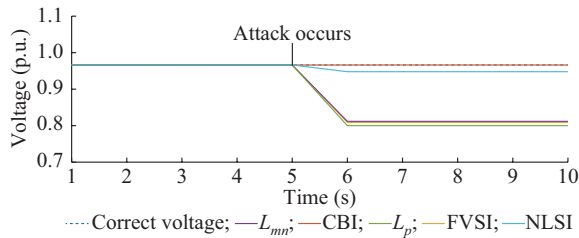


Fig. 8. Temporal evolution of the minimum bus voltage in Scenario B.

Importantly, as shown in Fig. 9, in Scenario A, the voltage stability indices themselves remain approximately unchanged (satisfying constraints (8) and (9)), making it difficult to detect the attack through conventional index monitoring despite the actual voltage drops shown in Fig. 7.

As shown in Fig. 8, Scenario B exhibits similar characteristics, with the proposed approach reducing voltage degrada-

tion by approximately 25% compared with conventional indices. Figure 10 shows that Scenario B represents a more sophisticated attack where the voltage stability indices appear improved (satisfying constraint (10) for conventional indices or (11) for CBI), creating a deceptive scenario where monitoring suggests enhanced stability while the actual bus voltages are decreasing. This discrepancy between apparently improved stability indices and the actual deteriorating voltages makes this attack particularly challenging to detect.

For the conventional indices shown in Figs. 9 and 10, values approaching zero indicate higher system stability, with values close to 1 signifying proximity to voltage collapse. Transmission line analysis based on Figs. 9 and 10 provides further insights into the performance of each index.

For Scenario A in Fig. 9, the results confirm that, for all transmission lines, the post-attack difference of each index stays below 0.1, satisfying the detection-avoidance constraint of Scenario A. Figure 9 primarily verifies that attacks successfully satisfy constraints (8) and (9) for all indices, demonstrating their ability to evade detection through conventional index monitoring.

The key benefit of CBI in terms of cybersecurity is not evident in Fig. 9, but rather in the constrained false data injection amounts, which will be quantitatively analyzed in subsequent figures. This demonstrates that while the actual bus voltages drop significantly, as shown in Fig. 7, the voltage stability indices remain nearly constant, validating the ability of attack to evade detection through conventional index monitoring.

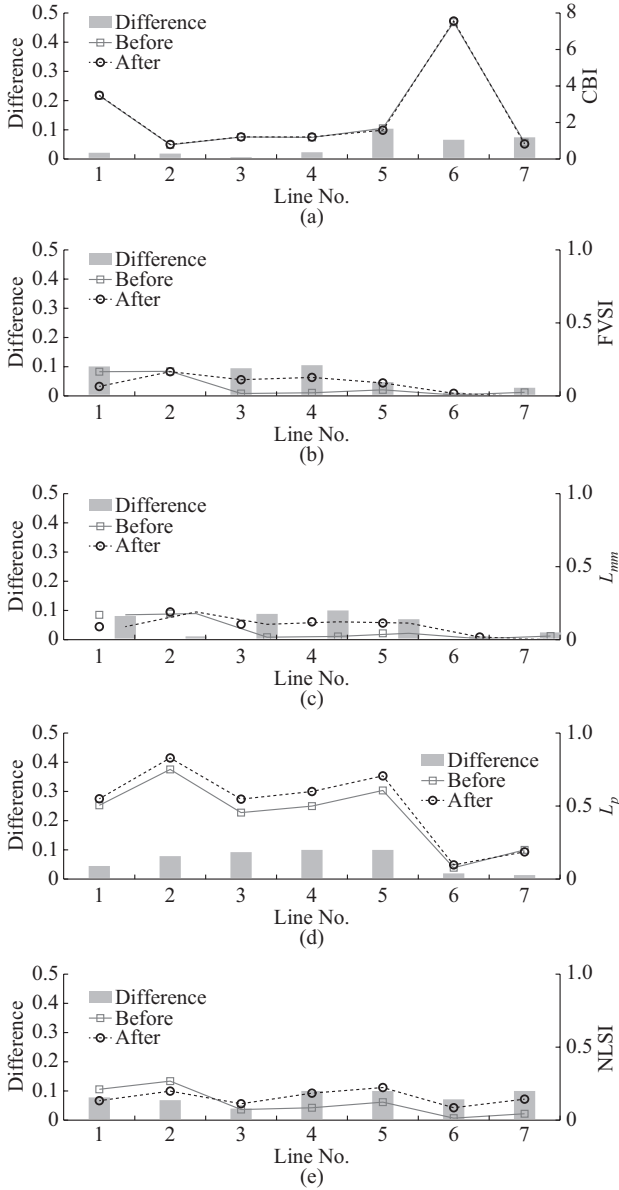


Fig. 9. Comparison of voltage stability indices for each transmission line before and after attack in Scenario A. (a) CBI. (b) FVSI. (c) L_{mn} . (d) L_p . (e) NLSI.

Notably, CBI demonstrates heightened sensitivity to the impacts of attacks compared with conventional indices, particularly in constraining the magnitude of false data that attackers can inject while maintaining apparent stability.

For Scenario B in Fig. 10, constraint conditions require post-attack index values to appear improved. The results confirm that these conditions are satisfied. For instance, Fig. 10(e) reveals significant apparent improvement in the NLSI index for transmission line 2, indicating targeted manipulation to create an artificially enhanced stability perception.

This apparent improvement in stability indices contrasts sharply with the actual deteriorating voltage in Fig. 8, highlighting the sophisticated nature of this camouflage attack and the challenge it poses for system operators who rely solely on conventional index monitoring.

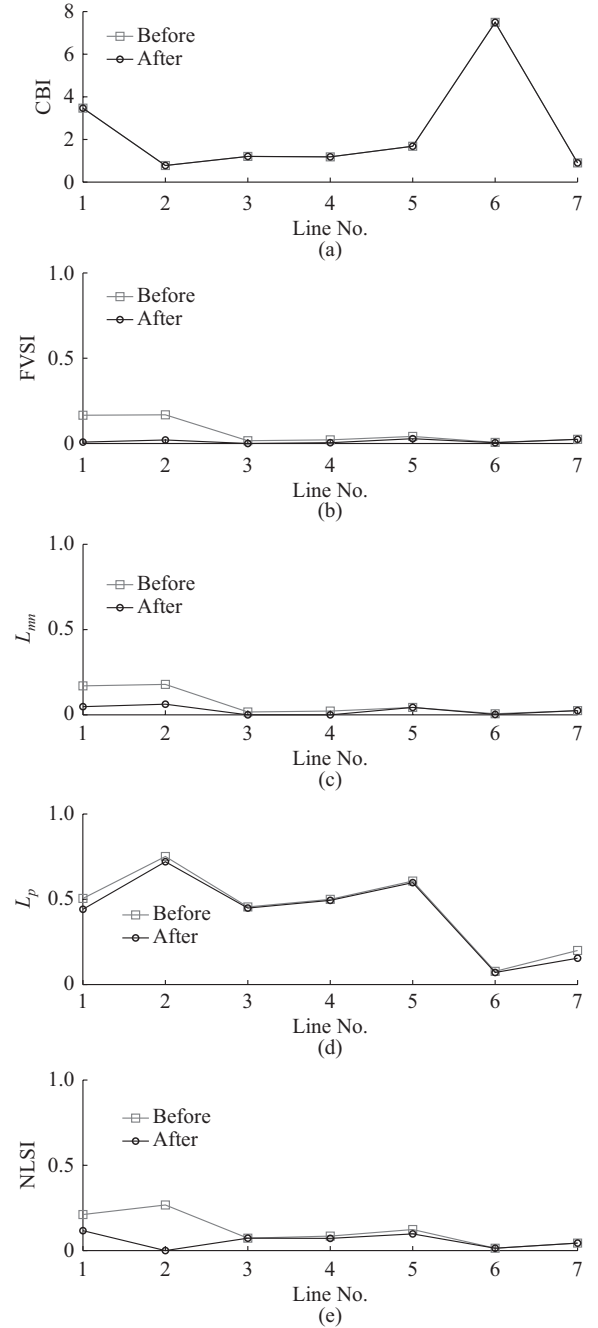


Fig. 10. Comparison of voltage stability indices for each transmission line before and after attack in Scenario B. (a) CBI. (b) FVSI. (c) L_{mn} . (d) L_p . (e) NLSI.

As shown in Figs. 11 and 12, quantitative analysis of the required false data injection amount reveals the substantial security advantage of the proposed approach, which represents the primary benefit of using CBI for system monitoring in the context of cybersecurity. When the proposed approach is employed, as shown in Fig. 11, injection quantities remain significantly constrained compared with conventional index L_p for monitoring, as shown in Fig. 12. In Scenario B, attackers targeting buses 3, 4, and 5 must limit manipulation to maximum values of ± 50 MW/Mvar under the proposed approach, whereas conventional monitoring allows manipulations up to ± 150 MW/Mvar. This three-fold reduction dem-

onstrates the enhanced sensitivity of the proposed approach to subtle data manipulations, effectively preventing attackers from implementing substantial measurement alterations and thereby suppressing potential voltage degradation. This preventive capability represents a fundamental advantage of CBI: the inherent characteristics of CBI force attackers to use significantly smaller injection amounts, which is directly translated to reduced voltage degradation and provides an additional layer of preventive defense.

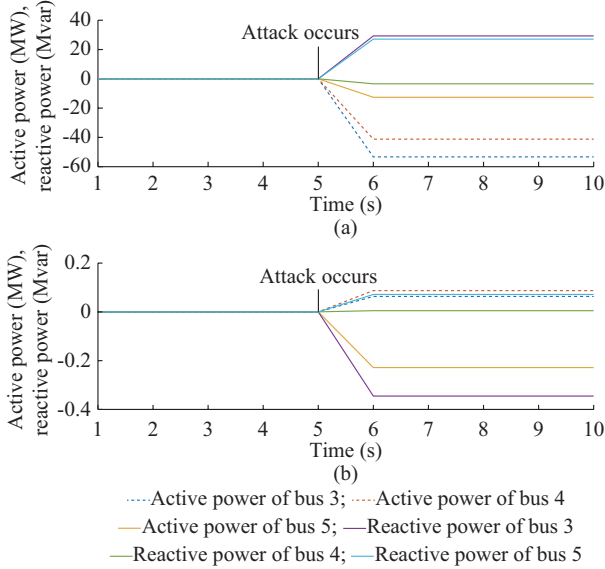


Fig. 11. False data injection amount when CBI is employed for monitoring. (a) Scenario A. (b) Scenario B.

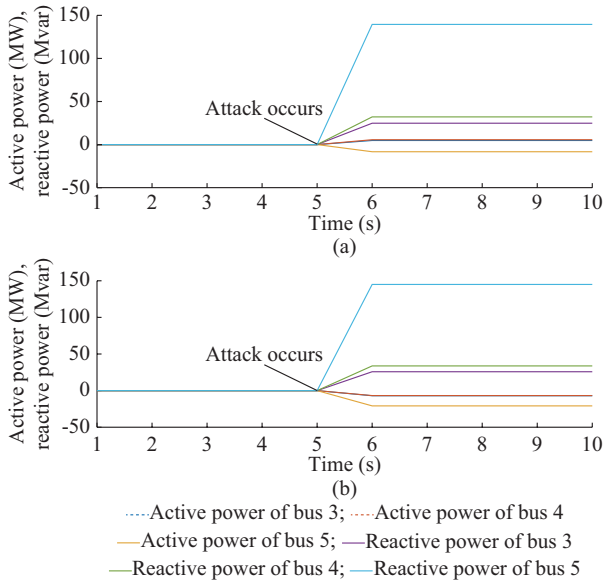


Fig. 12. False data injection amount when L_p is employed for monitoring. (a) Scenario A. (b) Scenario B.

C. Verification in Modified IEEE 118-bus Test System

A more practical verification is conducted using the modified IEEE 118-bus test system. As shown in Fig. 6, DERs are installed at various points in the system, and simultaneous attacks on different locations are assumed.

In this subsection, we evaluate the detection sensitivity of

each VSI, which is defined as the absolute difference between pre-attack and post-attack index values, i.e., $|VSI(P_{false}, Q_{false}) - VSI(P_{true}, Q_{true})|$. This metric corresponds directly to the left-hand side of constraint (8) in Scenario A. A larger difference indicates higher sensitivity to data manipulation, enabling earlier detection of attacks. By comparing the detection sensitivity across different indices, we can assess their relative effectiveness in identifying sophisticated FDIAs.

Figure 13 presents the detection sensitivity comparison of voltage stability indices during simultaneous attacks on buses 5, 15, and 20. The horizontal axis indicates transmission line numbers, while the vertical axis represents the detection sensitivity (i.e., the absolute difference in index values before and after the attack). Analysis reveals that CBI effectively identifies local anomalies even in complex large-scale systems. The transmission section between lines 40-60 exhibits particularly pronounced changes, indicating the vulnerability of this corridor to the simulated attack. Quantitative comparison shows that the proposed approach demonstrates approximately twice the sensitivity at attack locations compared with conventional indices, enabling the detection of subtle system changes.

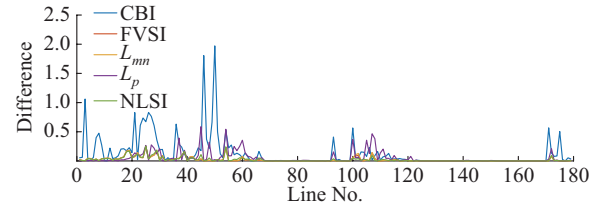


Fig. 13. Detection sensitivity comparison of voltage stability indices during simultaneous attacks on buses 5, 15, and 20.

Similar patterns emerge in Figs. 14 and 15, which illustrate responses to simultaneous attacks on buses 50, 55, 60 and buses 85, 95, 105, respectively. In Fig. 14, while all indices register some deviations around transmission lines 60-100, the proposed approach exhibits substantially more pronounced responses. Notably, CBI captures deviations in transmission corridors where conventional indices register minimal changes, highlighting its enhanced sensitivity to subtle system changes.

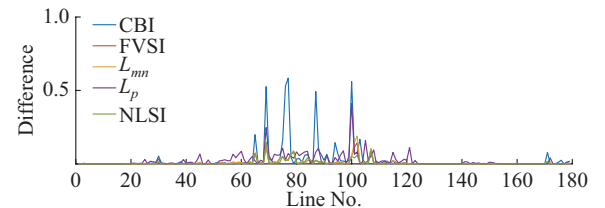


Fig. 14. Detection sensitivity comparison of voltage stability indices during simultaneous attacks on buses 50, 55, and 60.

The simultaneous attacks on buses 85, 95, and 105 in Fig. 15 produce localized impacts around transmission line 120, demonstrating how FDIAs can concentrate effects in specific network sections. In this case, the proposed approach demonstrates approximately 1.5 times greater sensitivity than conventional indices, accurately identifying the affected trans-

mission corridors.

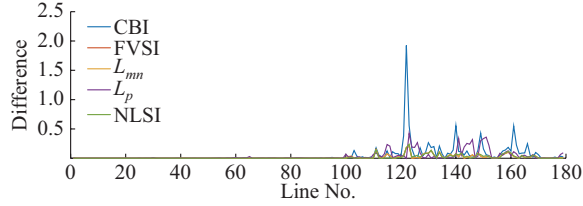


Fig. 15. Detection sensitivity comparison of voltage stability indices during simultaneous attacks on buses 85, 95, and 105.

A fundamental factor contributing to the superior sensitivity of the proposed approach lies in its measurement scale. While conventional indices operate within a normalized range of 0 to 1, CBI employs per-unit values to quantify deviations from the stability boundary. This scaling difference enables the representation of subtle system changes with proportionally larger numerical variations, effectively amplifying the detection capability for subtle manipulations, which is a critical advantage for monitoring sophisticated attacks designed to remain below conventional detection thresholds.

These findings confirm the consistent performance of the proposed approach across diverse system scales. The ability to precisely locate anomalies and identify affected components in increasingly complex networks represents a significant advancement for practical implementation. Furthermore, the demonstrated effectiveness against simultaneous multi-location attacks, which is a realistic threat scenario, underscores the operational value for securing modern power systems.

D. Comparison with State-of-the-art Approaches

To contextualize the proposed approach within the current research landscape, Table IV compares the proposed approach with state-of-the-art approaches, including ML-based and index-based approaches. In Table IV, VSI includes the FVSI, L_{mn} , L_p , and NLSI indices. It is important to note that these two categories address different aspects of cybersecurity. ML-based approaches focus on detecting attacks after they occur, while index-based approaches provide preventive resistance by limiting the attack effectiveness.

TABLE IV
COMPARISON OF PROPOSED APPROACH WITH STATE-OF-THE-ART APPROACHES

Category	Approach	Training required	Detection accuracy (%)	The maximum injection (MW/Mvar)	The minimum voltage (p.u.)
ML-based	DLSC [20]	Yes	99		
	GNN [10]	Yes	98		
Index-based	VSI	No		± 150	About 0.80
	CBI	No		± 50	> 0.95

Table IV reveals complementary strengths between ML-based approaches and the proposed approach. Recent ML-based approaches achieve high detection accuracy. Reference [20] reports detection accuracy of 99% using their deep latent space clustering (DLSC) on IEEE 118-bus test system,

while [10] achieves detection accuracy of 98% with their GNN-based approach on the Iberian 486-bus system. However, these approaches require training phases with historical data and detect attacks after they have been launched. In contrast, the proposed approach provides preventive defense by inherently constraining attacker capabilities without requiring any training. As demonstrated in Figs. 11 and 12, CBI limits the false data injection to ± 50 MW/Mvar compared with ± 150 MW/Mvar for conventional index L_p , a three-fold reduction in attack capability. This injection constraint directly translates to improved voltage stability. CBI maintains the minimum bus voltage above 0.95 p.u., even in Scenarios A and B shown in Figs. 7 and 8, whereas conventional indices allow voltage drops to approximately 0.8 p.u., approaching unstable operating regions.

The proposed approach offers three key advantages over existing approaches. ① No training requirement: unlike ML-based approaches achieving detection accuracy of more than 98%, CBI operates without training or labeled data, enabling immediate deployment. ② Preventive protection: CBI limits attack impact before detection by reducing the injection capability of attacker by 66%, complementing post-attack detection approaches. ③ Enhanced sensitivity: as shown in Figs. 13-15, CBI exhibits 1.5-2 times higher detection sensitivity compared with conventional indices, enabling earlier identification of sophisticated attacks. These results suggest that a multi-layer defense strategy combining preventive resistance (CBI) with post-attack detection (ML-based approaches) offers comprehensive protection against voltage stability attacks. CBI provides the first line of defense by limiting what attackers can achieve, while ML-based approaches serve as a secondary layer to identify attacks that bypass initial defenses.

V. CONCLUSION

This paper proposes a CBI-based preventive and post-detection defense approach against FDIAs in power systems with DERs, and evaluates its effectiveness through comprehensive simulation. The main findings are summarized as follows.

1) Verification using the modified IEEE 5-bus test system demonstrates that the proposed approach outperforms conventional indices such as FVSI, L_{mn} , L_p , and NLSI in attack detection. Using the proposed approach, intentional voltage drops are suppressed by approximately 25% compared with conventional indices. Furthermore, the analysis reveals that attackers require significantly smaller data manipulation quantities to achieve their objectives when CBI is employed. These results confirm the enhanced sensitivity of the proposed approach to minor data injections, which is a critical characteristic for attack prevention.

2) Application to the modified IEEE 118-bus test system validates the effectiveness of the proposed approach in large-scale networks. CBI-based monitoring successfully identifies the affected transmission lines even during simultaneous attacks at multiple locations. Quantitative analysis shows 1.5-2 times higher detection sensitivity compared with conventional indices, particularly for subtle system changes. This capa-

bility to precisely localize attack impacts to specific network sections (e.g., the transmission line 20-40 corridor or the vicinity of line 150) provides substantial operational value in complex power systems.

3) Cross-scale verification confirms the consistent performance of the proposed approach across different system scales, particularly its effectiveness against sophisticated camouflage attacks such as Scenario B that artificially improve stability indices to evade detection. The proposed approach, which monitors changes in system state rather than absolute index values, demonstrates superior resilience against sophisticated manipulation attempts compared with conventional indices.

These findings indicate that the preventive strategy offered by the proposed approach effectively complements conventional approaches, enhancing the comprehensive cybersecurity. This preventive paradigm particularly excels at limiting attack impacts before they propagate through the system, thereby improving the overall resilience.

Future research directions include investigating diverse attack patterns and developing real-time detection algorithms. Priority areas encompass the development of comprehensive monitoring techniques that leverage multiple stability indices, integration with machine learning-based anomaly detection, and formulation of multi-layered defense strategies. Additionally, including dynamic simulation would provide more comprehensive insights into system behavior during attacks. Distinguishing between legitimate DER variability and malicious FDIAs, leveraging grid code constraints, and analyzing temporal patterns also warrant further investigation. Finally, addressing emerging vulnerabilities associated with DER expansion represents an important research direction.

REFERENCES

- [1] C. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.
- [2] C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: state-of-the-art," *International Journal of Electrical Power and Energy Systems*, vol. 99, pp. 45-56, Jul. 2018.
- [3] G. Liang, S. R. Weller, J. Zhao *et al.*, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, Jul. 2017.
- [4] J. Beerman, D. Berent, Z. Falter *et al.*, "A review of colonial pipeline ransomware attack," in *Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops*, Bangalore, India, May 2023, pp. 8-15.
- [5] A. Vosughi, A. Tamimi, A. B. King *et al.*, "Cyber-physical vulnerability and resiliency analysis for DER integration: a review, challenges and research needs," *Renewable and Sustainable Energy Reviews*, vol. 168, p. 112794, Oct. 2022.
- [6] L. Garza, P. Mandal, and G. Ravikumar, "Cyber-attacks in inverter-based islanded microgrids considering DER dynamics," in *Proceedings of the 2024 56th North American Power Symposium*, El Paso, USA, Oct. 2024, pp. 1-6.
- [7] L. Garza, P. Mandal, and G. Ravikumar, "Mitigation of cyber attacks in DER-integrated distribution grid using deep generative models," in *Proceedings of the 2024 IEEE PES General Meeting*, Seattle, USA, Jul. 2024, pp. 1-5.
- [8] J. V. Notes. (2022, Aug.). CONTEC SolarView compact vulnerable to insufficient verification in uploading files. [Online]. Available: <https://jvn.jp/en/vu/JVNVU93696585/>
- [9] M. Egan, "A retrospective on 2022 cyber incidents in the wind energy sector and building future cyber resilience," Boise State University, Tech. Rep., Dec. 2022.
- [10] S. R. Fahim, R. Atat, C. Kececi *et al.*, "Graph neural network-based approach for detecting false data injection attacks on voltage stability," *IEEE Open Access Journal of Power and Energy*, vol. 12, pp. 12-23, Jan. 2025.
- [11] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, May 2018.
- [12] M. Furukakoi, O. B. Adewuyi, M. S. S. Danish *et al.*, "Critical boundary index (CBI) based on active and reactive power deviations," *International Journal of Electrical Power and Energy Systems*, vol. 100, pp. 50-57, Sept. 2018.
- [13] Z. Wu, H. Zhang, L. Jiang *et al.*, "Distributed unsupervised detection for robust power system false data attacks via flexible dynamic time warping strategy," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 1, pp. 277-286, Jan. 2025.
- [14] X. Li, W. Jiao, Q. Han *et al.*, "Detection of FDIA in power grid based on hypergraph and attention mechanism," *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 1862-1871, Jan. 2025.
- [15] M. Liu, X. Zhang, R. Zhang *et al.*, "Detection-triggered recursive impact mitigation against secondary false data injection attacks in cyber-physical microgrid," *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 1744-1761, Mar. 2025.
- [16] M. Rahman, J. Yan, and E. T. Fapi, "Adversarial artificial intelligence in blind false data injection in smart grid AC state estimation," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 6, pp. 8873-8883, Jun. 2024.
- [17] R. Sharikabadi, A. Abdollahi, M. Rashidinejad *et al.*, "Security constrained unit commitment in smart energy systems: a flexibility-driven approach considering false data injection attacks in electric vehicle parking lots," *International Journal of Electrical Power and Energy Systems*, vol. 161, p. 110180, Oct. 2024.
- [18] D. Tang, J. M. Guerrero, and E. Zio, "Securing demand-response in smart grids against false pricing attacks," *Energy Reports*, vol. 12, pp. 892-905, Dec. 2024.
- [19] T. Bragatto, M. A. Bucarelli, M. S. Bucarelli *et al.*, "False data injection impact on high RES power systems with centralized voltage regulation architecture," *Sensors*, vol. 23, no. 5, p. 2582, Feb. 2023.
- [20] A. Bhattacharjee, A. K. Mondal, A. Verma *et al.*, "Deep latent space clustering for detection of stealthy false data injection attacks against AC state estimation in power systems," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2338-2351, May 2023.
- [21] M. Zadsar, A. Abazari, A. Ameli *et al.*, "Prevention and detection of coordinated false data injection attacks on integrated power and gas systems," *IEEE Transactions on Power Systems*, vol. 38, no. 5, pp. 4252-4268, Sept. 2023.
- [22] M. Ismail and T. Rahman, "Estimation of maximum loadability in power systems by using fast voltage stability index (FVSI)," *International Journal of Power and Engineering Systems*, vol. 25, pp. 181-189, Oct. 2005.
- [23] M. Moghavvemi and F. Omar, "Technique for contingency monitoring and voltage collapse prediction," *IEE Proceedings - Generation, Transmission and Distribution*, vol. 145, no. 6, pp. 634-640, Nov. 1998.
- [24] M. Moghavvemi and M. Faruque, "Technique for assessment of voltage stability in ill-conditioned radial distribution network," *IEEE Power Engineering Review*, vol. 21, no. 1, pp. 58-60, Jan. 2001.
- [25] A. Yazdanpanah-Goharrizi and R. Asghari, "A novel line stability index (NLSI) for voltage stability assessment of power systems," in *Proceedings of the 7th WSEAS International Conference on Power Systems*, Beijing, China, Sept. 2007, pp. 164-167.
- [26] S. Balamurugan, S. Ashwin, C. S. Vaishnavi *et al.* (2022, Nov.). Big data from actual IEEE 5 bus system during normal and control operations. [Online]. Available: <https://ieee-dataport.org/documents/big-data-actual-ieee-5-bus-system-during-normal-and-control-operations>
- [27] R. D. Zimmerman and C. E. Murillo-Sánchez. (2025, Jan.). MATPOWER: steady-state power system simulation and optimization software. [Online]. Available: <https://matpower.org>

Masahiro Furukakoi received the B.S., M.S., and Ph.D. degrees from the University of the Ryukyus, Okinawa, Japan, in 2016, 2018, and 2021, respectively. In 2018, he joined the Hitachi Zosen Corporation, Osaka, Japan. In 2023, he joined the National Institute of Technology, Sasebo College, Sasebo, Japan. In 2024, he joined Sanyo-Onoda City University, Yamaguchi, Japan, where he is currently an Assistant Professor. His research interests include power system, renewable energy, and energy management.

Akito Nakadomari received the B.S., M.S., and Ph.D. degrees from the University of the Ryukyus, Okinawa, Japan, in 2020, 2022, and 2024, respectively. In 2024, he joined Saitama University, Saitama, Japan, where he is currently an Assistant Professor. His research interests include power system optimization and energy management.

Akie Uehara received the B.S., M.S., and Ph.D. degrees in electrical and electronics engineering from the University of the Ryukyus, Okinawa, Japan, in 2009, 2011, and 2013, respectively. In 2011, she joined the Okinawa Electric Power Company, Inc., Okinawa, Japan, and in 2025, she joined the University of the Ryukyus, where she is currently an Assistant Professor. Her current research interests include wind power generation system, power system, and energy management.

Paras Mandal received the Ph.D. degree in electrical engineering from the University of the Ryukyus, Okinawa, Japan, in 2005. He is currently the Director of the Power and Renewable Energy Systems (PRES) Laboratory and a Professor of electrical and computer engineering with The University of Texas at El Paso, El Paso, USA. His current research interests include electrified transportation, application of artificial intelligence and machine learning to power system, forecasting, electricity market operation, and data-driven algorithm for cyber-physical system.

Mitsunaga Kinjo received the B.E. degree in electrical and information engineering from the University of the Ryukyus, Okinawa, Japan, in 1996, and the M.E. degree in electrical engineering and the Ph.D. degree in information science from Tohoku University, Sendai, Japan, in 1998 and 2001, respectively. From 2001 to 2003, he was a Researcher in the PRESTO program of the Japan Science and Technology Corporation (JST) conducted by Dr. Shigeo Sato at Tohoku University. From 2003 to 2006, he was a Research Fellow of the Research Institute of Electrical Communication (RIEC), Tohoku University. In 2006, he joined the University of the Ryukyus, where he is currently an Associate Professor. His research interests include neuromorphic computing, quantum computation algorithm, and their hardware implementation and application to combinatorial optimization problem.

Tomonobu Senjyu received the B.S. and M.S. degrees in electrical engineering from the University of the Ryukyus, Okinawa, Japan, in 1986 and 1988, respectively, and the Ph.D. degree in electrical engineering from Nagoya University, Nagoya, Japan, in 1994. He is currently a Full Professor with the Department of Electrical and Electronic Engineering, University of the Ryukyus. He is currently serving as a Member for the Science Council of Japan. He is an IEEJ Fellow and AAIA Fellow. His research interests include renewable energy, power system optimization and operation, power electronics, and advanced control of electrical machine.