Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Tiered FDI Detection Method in AC State Estimation Coupled with Distributed Partitioning Approach

Om Rishi

omrishi07@gmail.com

Indian Institute of Technology

Dr. Ravi Yadav

Indian Institute of Technology

Research Article

Keywords: Cyber-Physical Systems, Distributed Partitioning State Estimation (DPSE), False Data Injection Attacks (FDIA), Hardware-in-the-Loop (HIL), Hybrid Error Model, Weighted Least Squares (WLS)

Posted Date: June 1st, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8916567/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Tiered FDI Detection Method in AC State Estimation Coupled with Distributed Partitioning Approach

Om Rishi[1*] and Dr. Ravi Yadav[1†]

[1*]Department of Electrical Engineering, Indian Institute of Technology, NH62, Jodhpur, 342030, Rajasthan, India.

*Corresponding author(s). E-mail(s): omrishi07@gmail.com;
Contributing authors: raviyee@iitj.ac.in;
†These authors contributed equally to this work.

Abstract

With the continuously rising interconnection of Distributed Generators (DGs) and utilization of communication infrastructure, the contemporary power distribution network is susceptible to advanced cyber-physical attacks and False Data Injection (FDI) attacks. In this paper, a comprehensive detection framework is introduced to protect the power grid's state estimation process against such cyber-attacks. An advanced Weighted Least Squares (WLS) state estimator incorporating a Hybrid Error Model is introduced to accurately model the measurement errors. These errors are proportionate to the actual measurement values. A tiered Bad Data Detection (BDD) method is employed to protect the power grid against collaborative and subtle attacks by employing Global Chi-Square, Normalized Residual, and Global Omega tests. In addition to the above, the proposed method addresses the subsequent scaling-up issue in electrical grids through the Distributed Partitioning State Estimation (DPSE), which identifies faults by zonal scoring of topological defects. This proposed framework is extensively validated using an IEEE 13-bus test feeder and a hardware-implemented Hardware-in-the-Loop (HIL) simulation environment. The simulation environment integrates a Typhoon HIL grid simulator and a Raspberry Pi platform, leveraging the accepted IEC 61850 MMS and IEC 60870-5-104 protocols. The experimental results demonstrate the effectiveness of the proposed solution for detecting and tracking FDI attacks as small as 10% of the active and reactive power.

Keywords: Cyber-Physical Systems, Distributed Partitioning State Estimation (DPSE), False Data Injection Attacks (FDIA), Hardware-in-the-Loop (HIL), Hybrid Error Model, Weighted Least Squares (WLS)

1 Introduction

The modernization of electrical power systems is increasingly defined by the widespread integration of Distributed Generators (DGs) and the deployment of advanced communication infrastructures. While this transition enhances grid efficiency and sustainability, it introduces significant cyber-physical vulnerabilities. The widespread deployment of Supervisory Control and Data Acquisition (SCADA) systems for grid monitoring and control significantly broadens the cyber-attack surface, thereby increasing susceptibility to malicious intrusions. Among various threats, False Data Injection Attacks (FDIAs) are among the most dangerous, as cyber attackers could use sensor measurements to deceive grid operators, leading to catastrophic blackouts, voltage instabilities, and/or uneconomic dispatches.

State Estimation (SE) is an integral part of grid defense, carried out to remove noise and obtain a true representation of the system's state. Bad Data Detection (BDD) is one of the most important functions of state estimation and deals with detecting irregularities in measurement data as well as data generated as a result of data injection. However, this effectiveness is fundamentally compromised by stealthy attacks that are specifically crafted to evade traditional statistical detection thresholds. In addition, the growing integration of high levels of distributed generators (DGs) into distribution networks introduces new challenges in terms of scalability for centralized estimation and the accurate modeling of measurement error areas, where conventional Weighted Least Squares (WLS) methods often fall short.

The existing literature has proposed various strategies to strengthen the microgrid resilience. Several studies have proposed resilient control frameworks for DGs and Energy Storage Systems (ESS) [1], [5] that focus on economic dispatch and frequency stability under attack conditions. However, these approaches tend to focus on control actions, overlooking the rigorous, multi-tiered BDD necessary to identify the source of data corruption. Other works have introduced distributed consensus protocols [2] and attack-resilient distributed control for AC microgrids [4], yet those studies repeatedly rely on simplified error models and lack the integration with standard industrial communication protocols. Some specific detection mechanisms, such as oscillator-based strategies [6] and observer-based methods for DC microgrids [3], have been developed, but they often fail to capture the hybrid nature of measurement errors, which combine fixed and proportional components of measurement value or the specific challenges of scaling detection across large and partitioned networks. Validation of these algorithms in Hardware-in-the-Loop (HIL) environments using real-world and industry-standard communication protocols, such as IEC 61850, remains largely unaddressed, which limits confidence in their deployment readiness.

To address these limitations, this paper proposes a comprehensive cyber-resilient detection and state estimation framework for the system. This paper introduces an

enhanced state estimator integrated with a Hybrid Error Model, which assigns weights to capture both fixed sensor noise and proportional measurement errors, thereby accurately representing the behavior of physical instrumentation. In order to combat stealthy and well-coordinated attacks, a hierarchical BDD approach is employed that combines the Global Chi-Squared Test, Normalized Residual analysis, and also the Global Omega Test. Moreover, Scalability is handled by a Distributed Partitioning State Estimation (DPSE) method that can identify faults within specific topological regions to prevent error smearing and improve localization accuracy.

Three key contributions are presented in this work. To improve estimation accuracy and detection sensitivity across a broad range of loading conditions, a realistic hybrid error model is first incorporated into the WLS formulation to jointly capture fixed and proportional sensor errors. Second, scalability is addressed using the Distributed Partitioning State Estimation (DPSE) technique, which divides the network topology into zones and effectively separates malicious data and hidden attacks that could have gone undetected with centralized methods. Finally, the experimental viability of the proposed framework has been demonstrated through a comprehensive evaluation on the IEEE 13-Bus Feeder system, developed on a Typhoon HIL platform, which integrates real-time grid simulations with the estimation logic using the IEC 61850 MMS and IEC 60870-5-104 communication protocols.

The rest of the paper is organized as follows: the System Modeling is explained in Section II. Section III explains the WLS framework, along with hybrid error modeling. In Section IV, the multi-tiered logic for bad data detection is discussed. The DPSE methodology is discussed in Section V, which is then followed by a description of the communication framework and HIL setup in Section VI. Section VII presents and analyzes the simulation results, with concluding remarks provided in Section VIII.

2 System Modeling and Framework

2.1 Network Model

For the validation of the proposed cyber-resilient model, the model is tested on the modified IEEE 13-bus test system, where the modifications were made to ensure realistic modeling and numerical consistency. The radial distribution test system is widely used to assess the performance of control schemes and estimation techniques. As a part of the proposed model for the sake of positive sequence state estimation, the original unbalanced multi-phase model is aggregated to form a balanced three-phase model. The model developed is based on the substation Node 632 as the reference node or the slack node with the Point of Common Coupling (PCC). Also, the developed model does not retain the same impedance as the original IEEE 13-bus model.

The network model also describes the physical connections between the system components and the line impedance parameters necessary for state estimation. The simulation environment used an open-source software called "OpenDSS" for the bus admittance (Y-bus) matrix and power flow analysis. The parameters of the system can be found in Table I.

The electrical network can be modeled using a Bus Admittance Matrix, which represents the electrical interconnections between the network nodes. The relationship

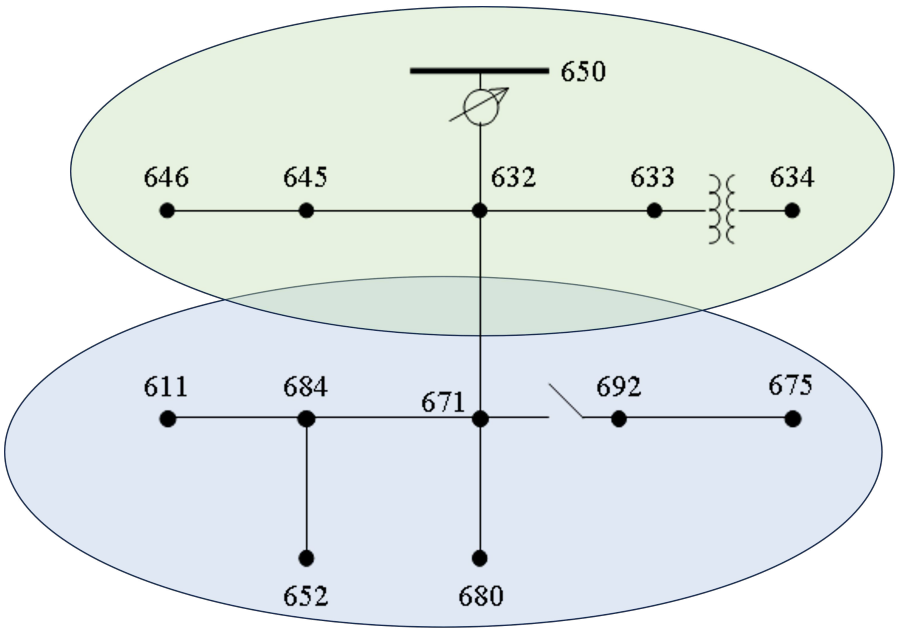


Fig. 1 Distributed IEEE 13 Node Test Feeder

Table 1 System Parameters

Parameters	Value	Unit
Number of Buses	12	–
Total Active load	1007.2	kW
Total Reactive load	487.8	kVAr
Total delivered active power	1030.5	kW
Total delivered reactive power	382.2	kVAr
Total real power loss	23.24	kW
System loss	2.3	%
Base voltage (primary)	6.351	kV
Base voltage (secondary)	2.402	kV
Transformer rating	500	kVA
Load power factor	0.9	–

between the injection of currents and voltages at the buses can be described by the equation:

$$I = Y_{Bus} \cdot V \tag{1}$$

The Bus admittance matrix is defined as:

$$Y_{bus} = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1n} \\ Y_{21} & Y_{22} & \cdots & Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{n1} & Y_{n2} & \cdots & Y_{nn} \end{bmatrix}$$

The diagonal elements Y_{ii} denote the self-admittance of the bus i, and the off-diagonal elements Y_{ij} represent the mutual admittance between the buses i and j.

For the purpose of state estimation, the system behavior is represented through a nonlinear measurement model. A baseline load flow simulation was performed to establish the "healthy" operating conditions. The total system active load is 1007.2 kW with a total reactive load of 487.8 kVAr. The simulation indicated total active power losses of 23.24 kW, which is approximately 2.3%, ensuring the model reflects realistic distribution loss characteristics.

2.2 Advanced Measurement Error Modeling

In the contemporary state estimation algorithm, the standard approach of assuming just one type of measurement error is no longer sufficient to accurately represent the nature of the instrumentation used in the field. For the WLS algorithm to approach the true solution, it is important to estimate the measurement error to the greatest level of reality possible. It is for this reason that the hybrid error approach is adopted.

Under this hybrid error model, each measurement is associated with a standard deviation σ that dictates how much weight is assigned to each specific reading during the estimation procedure. The model is mathematically expressed as:

$$\sigma = \sqrt{(\sigma_{\%} \times \text{reading})^2 + (\sigma_{\text{fixed}})^2} \tag{2}$$

Proportional Error ($\sigma_{\%} \times$ reading): This component symbolizes the "percent of reading" type of error. This type of error takes into account errors that grow according to scale, in other words, linearly according to the value of the measured quantity. For example, gain errors of potential transformers and current transformers. With a rise in the value of the measured quantity, this type of error will increase proportionally.

Fixed Error (σ_{fixed}): This measures the "percent of full scale" error. It differs from the proportional component because this component of the total error does not change based on the instantaneous value of the measurement being taken. In terms of system implementation, this component measures the constant noise floor of the data acquisition system, which corresponds to electronic thermal noise, Analog-to-Digital Converter errors, and errors incurred during communication transmission.

This is a better model than the simple ones because it better reflects the physical reality of how sensors actually perform across their full dynamic range. A model based purely on either percentage or fixed error is not an accurate model of the meter's performance across the full range of its use, because the blended model captures the major sources of uncertainty in measurement devices.

The strength of the hybrid model comes from its adaptability for different operation points, since in these cases two different regimes are responsible for the weighing of measurements in the WLS objective function. In the high-magnitude region, the

proportional part of the function prevails; at the same time, the fixed part becomes insignificant, helping scale the variance to prevent overconfidence in high-magnitude measurements. On the contrary, in the low-magnitude region, the proportional error becomes zero, and the fixed part introduces a constant error floor, thereby avoiding the numerical instability associated with infinite weights characteristic of proportional methods.

2.3 Attack model and Problem Statement

The increased resilience of SCADA and digital communication has significantly enhanced the observability and automation of modern grids. But this dependence has added vulnerabilities, particularly False Data Injection Attacks (FDIAs). Conventional State Estimation Frameworks, which are based on weighted Least Squares (WLS), are limited in their ability to scale with network size and local compromised measurements, and to maintain robustness under measurement uncertainty and Cyber attacks.

The primary objective is to reliably detect the presence of malicious data, accurately identify the affected network zones, and isolate the corrupted measurements from the SCADA estimation without compromising observability. Also, the computation must be efficient and resilient to measurement noise, modeling uncertainties, and communication constraints inherent in practical deployments.

We know that the non-linear measurement model is expressed as:

$$z = h(x) + e \tag{3}$$

where z denotes the measurement vector, x represents the states, and $h(.)$ and e are the non-linear measurement function and measurement noise by the error model, respectively.

Under the False Data Injection Attack, the compromised measurement vector is modeled as

$$z_a = z + a \tag{4}$$

where a is the malicious attack vector injected into selected measurements. The attack vector affects the measurements corresponding to the localized network region, creating correlated anomalies. It is assumed that the attacker has partial knowledge of the measurement structure but does not possess complete access to the system.

3 Centralized State estimation Framework

3.1 Weighted Least Squares

The essence of the state estimation process lies in attempting to arrive at the best possible estimate of the power system's static state vector, which is generally taken as a set of voltage magnitudes and phase angles at all buses in the network, given a set of redundant and noisy measurements of the same. Although various algorithms have been developed, the WLS method remains the foundational technique because it effectively filters measurement errors at sufficiently high redundancy.

The relation between the available measurements and the system state variables can be modeled by the nonlinear measurement equation:

$$z = h(x) + e \tag{5}$$

where z represents the measurement vector (comprising data such as power flows P_{ij}, Q_{ij}, bus injections P_i, Q_i, and voltage magnitudes $|V|$), x is the state vector to be estimated, and $h(x)$ is the nonlinear function relating the states to the measurements. The vector e accounts for measurement errors, which are generally assumed to be independent, Gaussian-distributed random variables with zero mean.

To solve for the unknown state vector x, the WLS method formulates the problem as an optimization task. We seek to minimize the weighted sum of the squared residuals, defined by the objective function:

$$J(x) = [z - h(x)]^T R^{-1} [z - h(x)] \tag{6}$$

Here, R is the measurement error covariance matrix. Typically, R is a diagonal matrix where each diagonal element R_{ii} corresponds to the variance σ_i^2 of the i-th measurement, reflecting the precision of the meter used.

$$R = \begin{bmatrix} \sigma_1^2 & 0 & \dots & 0 \\ 0 & \sigma_2^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_m^2 \end{bmatrix} \tag{7}$$

The measurement function h(x) is a nonlinear function involving trigonometric terms because of the power flow equations. A direct solution is not possible for h(x). We use an iterative approach with a solution following the Gauss-Newton algorithm. The linearization around the current solution point x^k is done with the help of a first-order Taylor series expansion.

To minimize the objective function, the gradient $g(x) = \partial J(x)/\partial x$ must be set to zero. Applying this optimality condition results in the following iterative update, which is commonly referred to as the normal equation:

$$G(x^k)\Delta x^{k+1} = H^T(x^k) R^{-1} [z - h(x^k)] \tag{8}$$

Here, $H(x)$ is the measurement Jacobian matrix, defined as $H = \partial h(x)/\partial x$, and $G(x) = H^T R^{-1} H$ is the Gain Matrix. The Gain Matrix is notably sparse, symmetric, and positive definite. These properties are exploited to enhance computational efficiency during the solution process.

The computational process of the WLS state estimator is formally expressed in Algorithm 1, which follows an iterative approach. Algorithm 1 requires the inputs of the measurement vector (z), the inverse weight matrix (R^{-1}), and the network topology models. At the start, the iteration counter, k, is initialized to zero with the state vector, x, starting with a "flat start" voltage of 1.0 p.u. and an angle of 0 degrees. During the iterative process, the state vector is transformed to the system representation, after which the measurement function of the nonlinear problem, $h(x)$, and the measurement Jacobian matrix, H, can be found. Then, the Gain Matrix G is

computed, for which its numeric non-singularity is checked explicitly. The algorithm then stops the iteration to prevent divergence and flags a numerical instability error if the matrix is singular. If the Gain Matrix is non-singular, the normal equations are solved to get the increment state correction vector Δx, whereupon the update $x \leftarrow x+\Delta x$ is made. The iterations continue until $\Delta x < \epsilon_{\text{tol}}$ for a pre-defined tolerance ϵ_{tol}. After convergence, the residual covariance matrix S is computed via the pseudo-inverse of the Gain Matrix. The matrix is key to subsequent bad-data identification processes, such as the Largest Normalized Residual test.

One major aspect of the WLS approach's efficiency is its sensitivity to the matrix weights, R^{-1}. In perfect conditions, specifying weights as inverses of measurement variances is advisable. Nevertheless, due to practical considerations, various measurements such as bus voltages and power injection are characterized with a difference in their sensitivity and contributions to estimation errors.

4 Bad Data Detection and Identification

Within the real world of power system operations, the correctness of State Estimation is under threat not only from the noisy nature of all measurements, which is commonly modeled as stochastic error (e), but also from "Bad Data" which represent large measurement outliers caused by faulty measurement instruments or biased telecommunication channels or even malicious cyber attacks. Although the Weighted Least Squares (WLS) method is robust against Gaussian error (e), it is very vulnerable to outliers ($|k|$). A contaminated measurement model can typically be expressed as:

$$z = h(x) + e + |k| \tag{9}$$

where, z is the measurement vector, $h(x)$ is the nonlinear function relating states to measurements, and $|k|$ represents the gross error component. If left unchecked, the WLS algorithm attempts to minimize the overall residual by "smearing" the error from the bad data point across healthy measurements, pulling the estimated state vector away from the true system operating point. It has been observed in practice that this often results in an erroneous control decision, like improper generator dispatch or a false security alarm.

4.1 BDD as two-step process

Now, the fundamental challenge in BDD is that the estimator only sees the measured value from the measuring instruments. The estimator itself has no way of knowing whether the measured value it receives is free of bad data. It also didn't know the cause of the error, i.e., either there is a sensor failure or false data is being injected into the system. The only way to highlight the bad data is by observing the residual. If the residual is larger than the set threshold value, this means there is a presence of bad data.

Bad Data detection is a two-step process:

- **STEP 1: Detection of Bad data**

During this process, the main objective is to check if there is any abnormal measurement data in the system. By calculating the residual vector after the WLS estimation process. The Global Chi-square test is used to identify the abnormality in the system. It basically performs the global statistical test for the same.

- **STEP 2: Identification of Bad Data**

If bad data is detected in the system, it needs to be located so that preventive action can be taken accordingly. The measurement, which is the problem for the system, is identified by the method of normalized residuals. If the maximum value of the normalized residual is more than the set threshold value, it will be flagged as bad data and will be removed. Now, when the bad data is removed, the state estimation is again implemented, and it is repeated again and again until all bad data is removed from the measurement vector.

The Detection and Identification should commence with a hierarchical method whereby, first, a statistical test would determine if the data set as a whole appears to be inconsistent. Following this, it would conduct tests to identify incorrect data points.

4.2 Global Chi Square test (χ^2-Test)

The chi-square test is essentially the first line of defense, the alarm trigger that goes off only when the total consistency of the measurement set is broken. This is essentially because there is a basic statistical theorem whereby the square of independent standard normal variables follows a Chi-Square distribution.

The test statistic, $J(\hat{x})$, is derived directly from the minimized WLS objective function. It represents the sum of the weighted squared residuals:

$$J(\hat{x}) = \sum_{i=1}^{m} \frac{(r_i)^2}{\sigma_i^2} = r^T W r \tag{10}$$

where $r = z - h(\hat{x})$ is the residual vector, $W = R^{-1}$ is the weight matrix, i.e., the inverse of the measurement error covariance matrix, and m is the total number of measurements.

Under the null hypothesis (H_0) that no bad data is present, $J(\hat{x})$ follows a χ^2 distribution with $k = m - n$ degrees of freedom, where n is the number of state variables. The detection logic relies on a threshold value $\chi^2_{(m-n),p}$ corresponding to a chosen confidence probability p (typically 0.95):

- If $J(\hat{x}) \leq \chi^2_{(m-n),p}$: The measurement set is consistent; H_0 is accepted.
- If $J(\hat{x}) > \chi^2_{(m-n),p}$: Bad data is suspected; H_0 is rejected.

The analysis of real-world implementations indicates that although computationally efficient, the Chi-Square test is significantly less reliable under certain conditions. If system redundancy, $m - n$, is low, then the statistical power of the test weakens. Moreover, the test is vulnerable to the "masking effect," in which multiple interacting bad data points effectively cancel each other out in the global sum, keeping $J(\hat{x})$ below the threshold despite severe corruption.

4.3 Normalized Residual Test (r_N-Test)

Once the global alarm is triggered, it is necessary to identify the specific source of the error. Also, it might be possible that the attacker has introduced false data in such a way that the Global Chi-Square test might fail to identify any abnormality in the system. That is why Identification tests are used as the second line of defence. Raw residuals (r_i) are poor indicators because they have very different variances and may be from quite different parts of the network topology. A bad measurement in a highly redundant area can easily produce small residuals across many sensors, the so-called "smearing effect" that precludes direct identification.

To overcome this, the normalized residual test was employed, which standardizes the residuals by their expected standard deviations. The normalized residual for the i-th measurement is given by:

$$r_{N,i} = \frac{|r_i|}{\sqrt{S_{ii}}} \tag{11}$$

Here, S_{ii} is the diagonal element of the residual covariance matrix S. The matrix S links the measurement errors to the residuals and is calculated as:

$$S = R - H(H^T W H)^{-1} H^T \tag{12}$$

where R is the measurement error covariance matrix and H is the Jacobian. The term S_{ii} represents the sensitivity of the residual to the error in the i-th measurement. In high-redundancy areas, S_{ii} tends to be small, which correctly amplifies the normalized residual for a given error.

The bad data identification procedure adopted in this work follows an iterative framework. At each iteration, the normalized residual ($r_{N,i}$) is computed for all measurements $i = 1, \ldots, m$, after which the measurement corresponding to the maximum normalized residual is identified as $idx_{max} = \text{argmax}(r_N)$. The maximum normalized residual $r_{N,max}$ is then compared against a predefined statistical threshold τ_{bdd}. If $r_{N,\text{max}}$ exceeds the set threshold value, that corresponding measurement is flagged as bad data, then removed from the measurement set, and the state estimation process is re-executed. This process is repeated till all remaining normalized residual values lie below the specified threshold, which indicates the absence of detectable bad data.

4.4 Global Omega (Ω_{ij}) Test

To overcome the drawbacks of coordinated attacks, especially because ordinary tests cannot model correlated error, and a faulty data point. So, for effective detection, the concept of the Global Omega (Ω_{ij}) Test must be introduced. In ordinary tests, only diagonal elements S_{ii} are needed because they are based entirely on the assumption that model data error is uncorrelated. In truth, however, they are very correlated via physical systems.

The Ω_{ij} test improves the detection metric by clearly taking in account for these correlations using the off-diagonal elements S_{ij}. The test statistic is formulated as:

$$\Omega_{ij} = \underbrace{\sum_{i} \frac{r_i^2}{S_{ii}}}_{\text{(chi-square part)}} + \underbrace{\sum_{\substack{i \neq j \\ |R_{r_n}(i,j)| > \tau_{\text{corr}}}} \frac{r_i r_j}{S_{ij}}}_{\text{(correlation cross-term part)}} \tag{13}$$

This equation has two components: the first term is the usual sum of squared normalized residuals; the second term is the "correlation cross-term". The latter is non-zero only when the pairs of measurements (i, j) are highly correlated, i.e. for $R_{r_n}(i, j) > \tau_{corr}$, for some threshold τ_{corr}. The coefficient is calculated as:

$$R_{r_n}(i, j) = \frac{S_{ij}}{\sqrt{S_{ii} S_{jj}}} \tag{14}$$

This dimensionless coefficient ranges from -1 to +1. A value near ± 1 indicates that the residuals are strongly linked.

Through the incorporation of these cross-terms, Ω_{ij} test effectively performs a "de-smearing" on the error. The test accounts for the possibility that an error in one data point may be due to an error in a strongly correlated neighboring data point. Comparison reveals that this test has up to 1.56 times greater detection capability for bad data points than the Chi-Square test, especially when data errors are small. Although it has higher computation complexity due to the computation of off-diagonal elements of γ, there is no objectionable reason not to use the Ω_{ij} test due to its stronger resistance to coordinated attacks.

An effective bad data detection method requires a multifaceted approach. The Global Chi-Square Test offers a necessary layer of data integrity verification, but it is not completely sufficient on its own. The Normalized Residual Test provides the level of detail needed to single out specific problems, but may fall victim to error smear for more complicated topologies. The Global Omega Test combines the strengths of the two in a sophisticated approach, utilizing statistical correlations to more effectively distinguish between the different interacting problems. The combination of the three provides an effective method to implement a high-fidelity state estimator.

5 Distributed Partitioning State Estimation (DPSE)

The Weighted Least Squares approach is a strong starting point for state estimation, but its extension to larger and more complex topological structures poses several challenges for scaling up. As noted in the initial simulations performed on the test case, the centralized solution is computationally demanding in nature. However, more importantly, it has a high likelihood of being affected by the 'smearing' phenomenon. As noted in a globally connected solution, even a flawed data point due to sensor failure or a targeted False Data Injection attack tends to distribute its error equally in its neighboring data elements.

To address these vulnerabilities, we extended the framework to include Distributed Partitioning State Estimation. This approach shifts the paradigm from a single, all-encompassing solution to a modular, partitioned strategy. By segmenting the grid into smaller, manageable zones, we can isolate faults geographically, enhance computational

efficiency through possible parallelization, and greatly improve the detectability of stealthy cyber-attacks that could otherwise be diluted within a global estimate.

5.1 Methodology and Grid Partitioning

In this study, the implementation of DPSE takes a hierarchical approach to provide a trade-off between global observability and regional accuracy. This begins with the power network being divided into k non-overlapping zones or sub-systems.

The strategy for partitioning is topology-based to ensure that there is a sufficient number of local measurements in each zone to maintain observability. In the case of our 12-bus system, different zones were established by interconnecting a tie-line. The essential component in this strategy is how it treats measurements of power flow in different tie-lines. Unlike traditional decentralized strategies, in which boundary measurements are exchanged iteratively to achieve consensus, this strategy treats power flow measurements in tie lines as boundary injections for the local estimators in both zones they interconnect.

Before the local estimators work, there is a standard WLS estimation for the global system to generate a state vector estimate x_{global}. This is necessary to have a "coarse" complete state description. Although this global state could have been affected by bad data due to smearing, it supplies enough boundary conditions for all local estimators. H refers to Jacobians, as well as weights W for the entire network and z is the measurement vector.

$$\hat{x}_{global} = (H^T W H)^{-1} H^T W z \tag{15}$$

Once the global baseline is obtained, the code produces a local estimation subproblem for each zone defined. For a given zone k, we define a local state vector x_k and a local measurement subset z_k that encompasses any internal sensors and the respective tie-line measurements.

The objective is to minimize the weighted sum of squared residuals for the zone, defined locally as:

$$J_k(x_k) = [z_k - h_k(x_k)]^T R_k^{-1} [z_k - h_k(x_k)] \tag{16}$$

Here, R_k^{-1} is the inverse covariance matrix specific to the measurements in zone k. This local objective function can be solved iteratively using the standard Gauss-Newton method independently for each zone.

At last, a key innovation in this implementation is Boundary Conditioning. The voltage magnitudes and phase angles for the boundary buses that connect Zone k to the rest of the grid are not estimated from scratch. Instead, they are fixed or tightly constrained using the values obtained from x_{global}. It is done because if each zone estimates the values independently, then the chances are that it may get inconsistency, leading to slow convergence and boundary mismatch errors.

$$x_{boundary} \leftarrow x_{global} \text{ (fixed)}$$

This approach is very effective at decoupling the domains. It supplies the local estimator with a fixed reference context to work within, so that it can simply concentrate on the consistency of its local measurements. When a domain has bad data, the local estimator, constrained by these boundaries, has no mathematical way to match the data to the model and creates very large local residuals or fails to converge.

5.2 Cyber-Resilience and Fault Isolation

The movement from a monolithic to a distributed architecture has its own set of advantages, recognized and realized during the validation procedure on the HIL testbed. In the solution to a global WLS problem, the estimator attempts to find a solution that minimizes the overall error $J(x)$ for all state variables. Consequently, an error indicated by a faulty sensor is often diffused or well distributed to other harmless sensors, keeping all their residuals just below the level of detection. In DPSE, on the other hand, the diffusion is constrained because of the 'wall' imposed by the boundaries of the zone regions. As tested, bad data that is well hidden in the solution is very evident in a local solution. A high value of the normalized residual variance in a local solution is a strong indicator of the source of the problems.

One of the most interesting results obtained during implementation is the behavior of the system in the case of joint attacks. When a "stealthy" FDIA is used by the attacker, and the attacker attempts to fraudulently convince the global estimator by slightly modifying a number of measurements (and in turn making the global χ^2 test successful), the "consistent" false reality created by the attacker collapses at the zonal interfaces. The local estimator for the attacked zone may not converge or get a Particularly High Zonal Anomaly Score ($Score_{zone}$) calculated as the sum of the squares of the normalized residuals in the zone:

$$Score_{zone} = \sum_{i \in \text{zone}} (r_{N,i})^2 \tag{17}$$

This metric functions as a localized Chi-Square test, detecting noisy regions even when individual measurements are not identified as gross errors. Although the 12-bus system is small enough to be handled by a single processor, the DPSE architecture is inherently run in parallel in different zones. The computational complexity goes down drastically because, by breaking the N-bus problem into k smaller problems of size N/k, WLS computational complexity scales super-linearly with the system size. These zonal estimators in a real-world utility deployment can therefore be run in parallel across distributed processors or edge devices and enable real-time monitoring of large distribution networks.

Therefore, the cyber-resilient framework is completed by the Distributed Partitioning State Estimation. While the Hybrid Error Model provides assurance that measurements will be weighted by their respective physical realities, and the global BDD tests form a first line of defense, the DPSE provides spatial resolution to isolate sophisticated attacks. It effectively eliminates the "smearing" weakness in traditional WLS, ensuring that a compromised sensor in a neighborhood cannot bring down the state awareness of the whole grid. This hierarchical approach-Global Pre-Estimation

followed by refined Zonal Analysis-forms the robust core of our defense strategy, the efficacy of which is illustrated in the subsequent results section.

6 Communication Framework and TestBed Architecture

For the purpose of validating the cyber-resilience of the proposed algorithms in a realistic environment, a hardware-in-the-loop (HIL) testbed has been implemented that models the hierarchical structure of the modern substation. The testbed allows the power system simulation to be separated from the estimation logic through additional communication layers, which naturally serve as potential attack points.

In this setup, the Typhoon HIL 402 serves as the physical plant, modeling the 12-bus distribution network in real time. Then, the Raspberry Pi is the data concentrator or Remote Terminal Unit (RTU), gathering process-level information. Finally, the host PC is the SCADA Control Center, in which the Weighted Least Squares (WLS) and Bad Data Detection (BDD) algorithms are implemented. Furthermore, this setup also enables the simulation of the False Data Injection (FDI) attack focused only on the communication channel between the RTU and the Control Center, which helps in verifying the estimator's capability to estimate the actual state from the malicious data set.

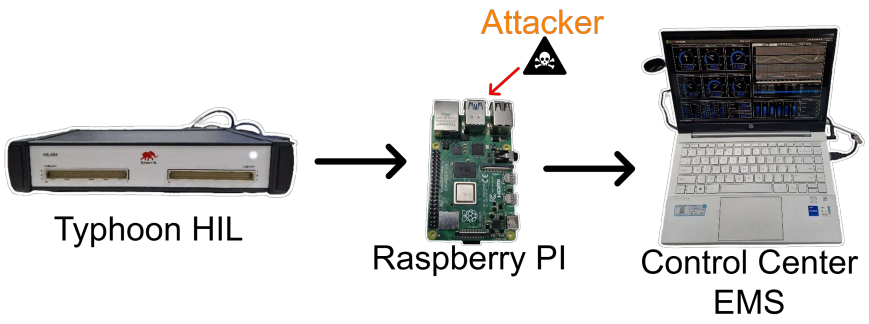


Fig. 2 Hardware-in-the-Loop (HIL) Experimental Setup with Attack injection Point

6.1 Substation Communication Protocol: IEC 61850 MMS

In the first-tier communication, the simulated grid and the data concentrator are connected. In this tier, the IEC 61850 Manufacturing Message Specification protocol is chosen based on the object-oriented approach, where the simulated measurements are organized as standardized logical objects instead of raw signals.

This protocol replicates the way devices communicate in real-time inside the substation. It has different logical levels, where the first is the process level. In this, sensors and actuators like CTs/ PTs, circuit breakers send the raw data samples digitally. The second is the Bay level, where protection relays, bay controllers, and local automation devices are operated. Also, the IEC 61850 has different message types:

- **GOOSE (Generic Object-Oriented Substation Event):** The purpose of this type is for fast protection signals, such as Trip Commands, interlocking, and fault signals. It does not use any TCP/IP protocol, which makes it very fast but less secure.
- **Sampled Values (SV):** It is used to stream the analog values of measurements like voltage waveforms and current waveforms. It is particularly used by the protection and control algorithms.
- **MMS (Manufacturing Message Specification):** To fulfill the purpose of configuration, monitoring, and control, MMS communication is used. This communication layer uses the TCP/IP protocol. This is slower than GOOSE and SV. It transmits the data, such as breaker status and changes in relay settings.

In the Typhoon HIL setup, the simulation model was set up as an IEC 61850 Server. The measurements have been referenced with the use of SCL files, involving a Configured IED Description, mapping the internal measurements to the MMXU (Measurement) logical nodes. In the quest for optimal bandwidth, the use of the "Report by Exception" mechanism is included, where the server will monitor the "mag.f" attribute of the Analog Values. The server will generate a report only when the measurement crosses a dead band threshold, $dbDelta$.

$$dbDelta = \frac{(max - min)}{100000} \times db \tag{18}$$

The Raspberry Pi, acting as the MMS Client, subscribes to this report. It breaks down the Data Sets received, retrieving the measured values, as well as their Quality (q) and Timestamp (t) attributes, thereby converting the physical parameters of the substation into their digital forms.

6.2 SCADA Telecontrol Protocol: IEC 60870-5-104

After that, the data will be aggregated at the Raspberry Pi and needs to be transferred to the Control Center (PC) for analysis. As for the wide-range data transmission, the use of the IEC 60870-5-104 protocol was implemented, which is one of the most widely used standards for SCADA communications over the TCP/IP network.

The Raspberry Pi is configured as the IEC 104 Controlled Station (Server), mapping the IEC 61850 data points to IEC 104 Information Object Addresses (IOA). It packages the measurements into Application Service Data Units (ASDUs) and transmits them over Ethernet to the SCADA.

The connection between the Raspberry Pi and the SCADA symbolizes the 'untrusted' network area where the cyber-attack is taking place. Prior to the data transmission to the estimation algorithms on the PC, an aggressor intercepts the IEC-104 message payloads and modifies the measurement values (injecting the vector $|k|$ into the measurement z). Such a configuration can be said to model a realistic attack environment where an aggressor has breached either the communication or the RTU and is sending spoofed measurement values to the grid managers.

6.3 Control Center Estimation (SCADA)

The destination of the data is the host PC, which acts as the Energy Management System (EMS). It acts as the Controlling Station/Client in the IEC 104 communication protocol and receives the endless flow of ASDUs. Upon receiving this data, the PC derives the measure vector z that includes both the system noise component e and the malicious attack signal component $|k|$. This contaminated data is subsequently used as an input into the state estimation tool implemented on the PC using Python scripts. It is here that the defense tools and strategies, as elucidated within the previous sections, including the Hybrid Error Model, Weighted Least Squares estimation, and multi-level Bad Data detection (Chi-Square, Normalized Residual, and Omega tests), are activated.

We moved the estimation logic to a PC downstream of the attack surface, where we could test this framework's ability to identify and sanitize data inconsistencies before they are used for critical grid monitoring, thereby emulating a cyber-resilient control center.

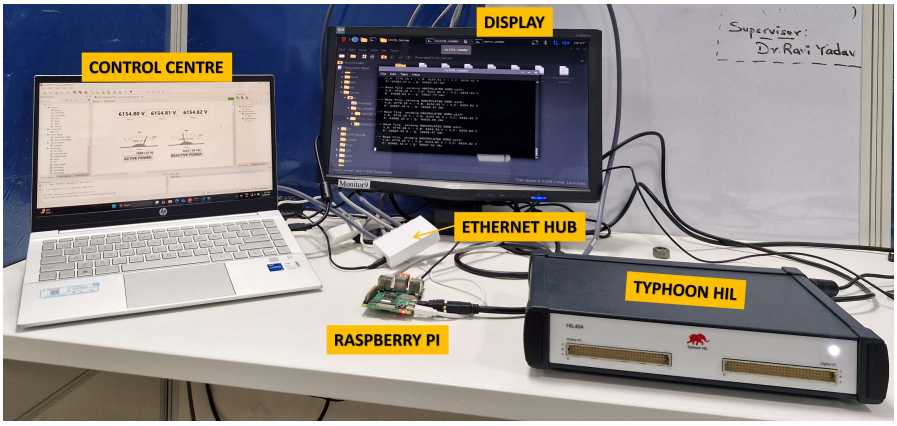


Fig. 3 Experimental setup showing the Typhoon HIL real-time power system emulator, Raspberry Pi edge gateway acting as a data concentrator, Ethernet-based communication network, and SCADA-based control center (EMS)

7 Results

To test the effectiveness and validity of the proposed framework, experiments were carried out on the Hardware-in-the-Loop (HIL) testbed. The main goal was to evaluate the performance in terms of detection capability and dynamic behavior when subjected to active False Data Injection (FDI) attack scenarios for the Weighted Least Squares (WLS) estimator and the Distributed Partitioning State Estimation (DPSE) technique.

The simulation scenarios were developed based on active and reactive power flow manipulations, with values varying between 10% and 20% of the measured raw values.

The following subsections highlight the performance of the system on detecting these anomalies, segregating the sensors, and using zonal analysis to provide scalable defense.

7.1 Estimator Performance Under FDI Attacks

The initial testing phase was based on the system's response to data corruption occurring at a sudden interval. The system response was evaluated based on the maximum normalized residual, indicating when data corruption is likely to happen.

7.1.1 Case 1: Attack on Active Power Flow

In the initial attack, the focus was on the active flow from Bus-632 to Bus-671. The attack involved the injection of the false measurements, whose amplitude was comparable to 10% of the amplitude of the original measurement. Looking back at the time-series values recorded during the attack, the system did not have any impact until the time of the attack, which was recorded at 19:52:57. The very next cycle after the attack was conducted, the maximum normalized residue, which was constantly around the baseline of approximately 184.21, was recorded to peak at 190.28.

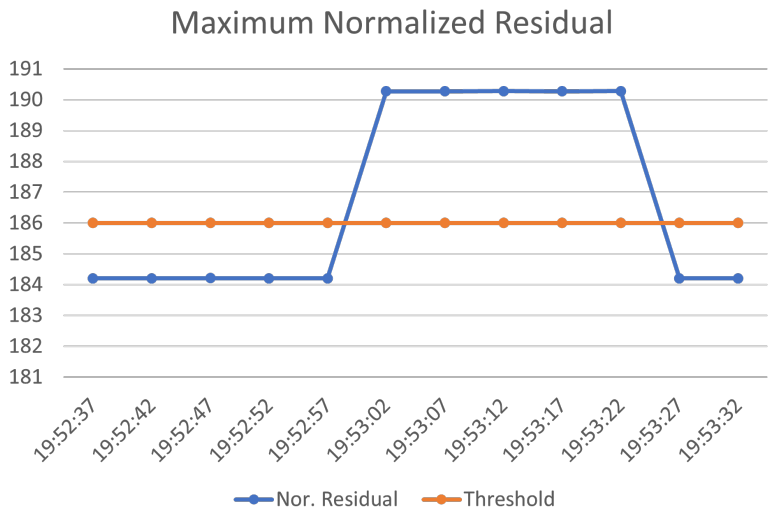


Fig. 4 Threshold behavior during FDI attack on active power flow (Bus-1 to Bus-8).

This spike triggered the WLS bad data logic. Immediately after the residual exceeded the predefined threshold, the algorithm raised the inconsistency flag. The estimator declared this corrupted measurement and removed it from the set of calculations. Thus, the normalized residual significantly fell back from the attack peak to 143.97, confirming that the bad data had been filtered out.

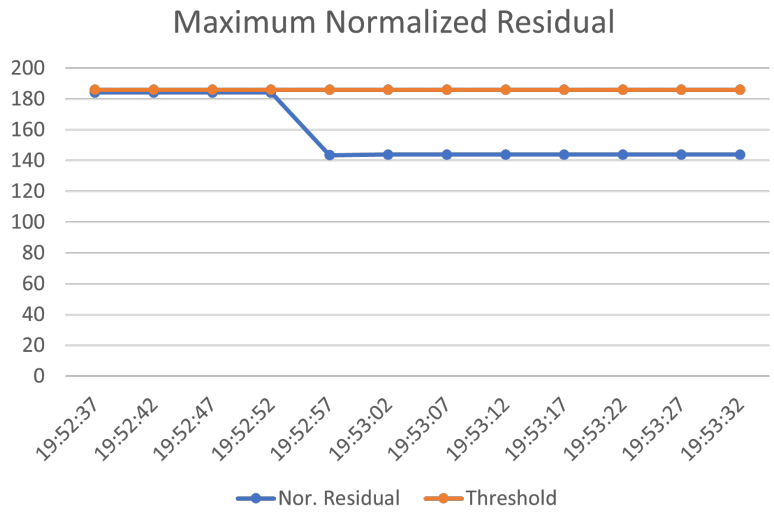


Fig. 5 Reduction in normalized residual following bad data removal by WLS.

7.1.2 Case 2: Attack on Reactive Power Flow

To validate the resilience characteristics of the proposed framework for a variety of measurements, we staged a further attack on the reactive power flow between the Bus-671 and Bus-680 nodes. For this more hostile attack, the false data injection value had been elevated to 20%. The system behavior remained the same. After the injection, the normalized residual value is observed to be 187.35, which is much farther away from the background noise. After the identification algorithm picked up the anomaly, the WLS algorithm removed the problem, and the residual value became a healthy 142.68.

7.2 Identification and Localization of Faulty Measurements

However, beyond mere detection, precise localization of the compromised sensor is one crucial requirement for cyber-resilience. The distribution of normalized residuals across the network gives insight into the location of the attack.

For the active flow attack scenario (Case 1), when residuals for different measurements of power flow were plotted, a striking difference stood out. Whereas most sensors showed only trivial deviations due to typical system noise and couplings, a statistically significant anomaly stood out in the particular measurement denoted "Pflow_8_6", clearly well beyond that of the other measurements. Its high value made it possible to pinpoint "Pflow_8_6" as the particular source of error, so that it could be removed without losing useful data from the rest of the system.

This same localization ability was also demonstrated in Case 2. The attack on the reactive flow caused a huge spike in the "Qflow_8_12" bar value, which was much larger than the residuals of the other nearby sensors. The above results have successfully validated the ability of the proposed framework to distinguish between the overall

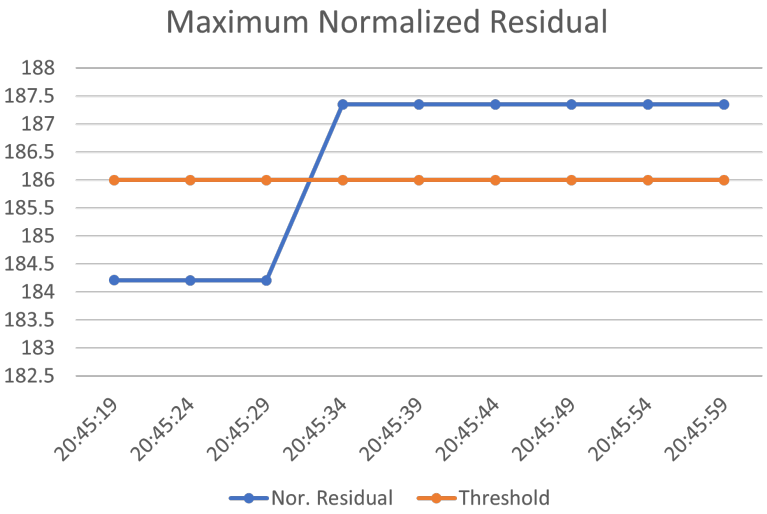


Fig. 6 Threshold behavior during FDI attack on reactive power flow (Bus-8 to Bus-12).

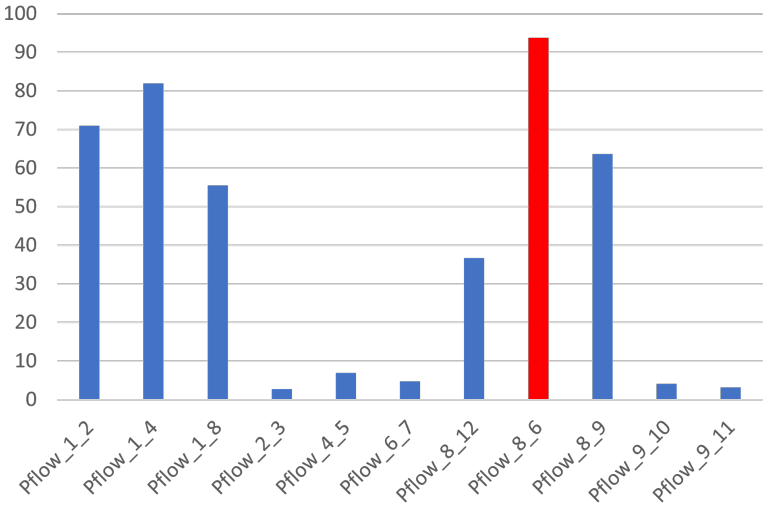


Fig. 7 Normalized residuals for power flow measurements, highlighting the attacked path.

noise in the system and sharp point-of-failure attacks to prevent the control center from considering false reports.

7.3 Scalability via Distributed Zonal Analysis (DPSE)

In studying the results when considering bigger systems, we noticed that pinpointing a sensor becomes computationally intensive as the size of the network increases. In

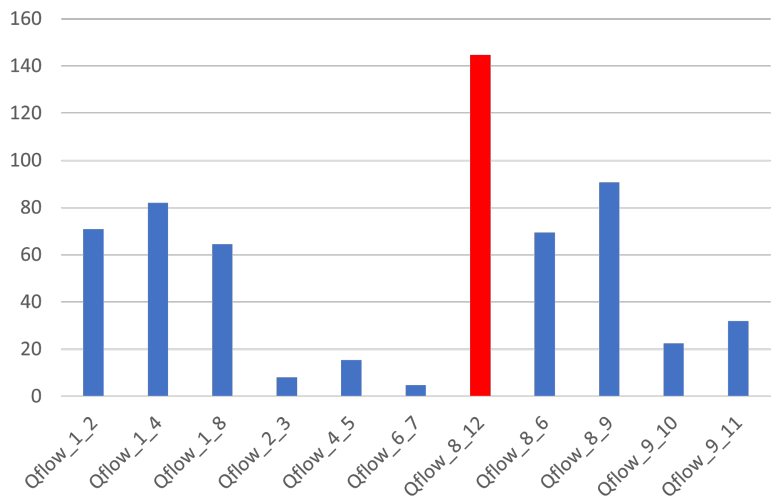


Fig. 8 Identification of faulty measurement Qflow_8_12 via residual analysis.

Table 2 DPSE Zonal Anomaly Detection Results

Zone	Converged	Norm. Residual	Threshold	Bad Data	Timestamp
Zone_1	TRUE	108.6559720	150.00	FALSE	21:16:38
Zone_1	TRUE	108.6564821	150.00	FALSE	21:16:43
Zone_1	TRUE	108.6561409	150.00	FALSE	21:16:48
Zone_1	TRUE	108.6561824	150.00	FALSE	21:16:53
Zone_2	TRUE	215.9521379	250.00	FALSE	21:16:38
Zone_2	TRUE	215.9522007	250.00	FALSE	21:16:43
Zone_2	TRUE	215.9523956	250.00	FALSE	21:16:48
Zone_2	TRUE	215.9516382	250.00	FALSE	21:16:53

this regard, the use of the Distributed Partitioning State Estimation (DPSE) strategy was found to be more efficacious and successful in coping with the challenges posed by complexity. In the hierarchical detection system, the 12-bus network was divided into two different areas, referred to as Zone 1 and Zone 2.

This partitioning effectively results in the "Post-Estimation Zonal Anomaly Detection" presented in Table I. As can be seen, during an attack sequence, there was a clear separation in the aggregate health of the zones: Zone 1 showed a consistently lower residual value of roughly 108, whereas Zone 2, containing the compromised measurement, remained steady with a higher residual value of about 215.

This is a very important gap because this allows the system to infer that Zone 2 is the stressed zone without having to assess all sensors at the same time. This sensitivity of the approach, which can detect zones of interest and perform local analysis, further supports the observation that the DPSE framework is efficient at reducing computational complexity without compromising accuracy. Also, once the compromised zone is identified, its measurements can be flagged and excluded from the SCADA state

estimation process, and control action can be implemented in the affected area to maintain the overall system stability and reliability.

8 Conclusion

In this work, we integrated the hybrid error model into the WLS algorithm and could successfully emulate realistic sensor behavior, substantially increasing the sensitivity of the BDD logic. Another important contribution of this work is the implementation of DPSE, which proved essential for scalability while effectively localizing stealthy attacks within specific topological zones that were otherwise masked in a monolithic global estimation.

Its practical efficacy was further verified on a real-time Hardware-in-the-Loop (HIL) testbed, emulating a digital substation architecture, on Typhoon HIL, Raspberry Pi, and industrial IEC 61850/IEC 60870-5-104 protocols. Experimental results have confirmed that the proposed approach is indeed capable of successful detection and rejection of active and reactive flow attacks of 10–20% magnitude, thereby maintaining state awareness under adversarial conditions. Future work will move from passive detection to active cyber-resilience by focusing on closed-loop control algorithms that dynamically re-dispatch Distributed Energy Resources (DERs) in order to compensate for compromised data. Validation on larger, multi-area networks will also be addressed.

Declarations

Funding

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Conflict of interest

The authors declare that they have no conflict of interest.

Ethics approval and consent to participate

This study did not involve human participants, animals, or any identifiable human data. Therefore, ethics approval and consent to participate were not required.

Consent for publication

The authors declare that this manuscript does not contain any individual person's data in any form.

Data availability

The datasets generated and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Materials availability

The hardware materials used in this study are commercially available.

Code availability

The code developed for this study is available from the corresponding author upon reasonable request.

Author contributions

Both authors contributed equally to the conceptualization, methodology development, implementation, analysis, and writing of the manuscript. Both authors reviewed and approved the final manuscript.

References

[1] W. Zhang, T. Qian, X. Chen, K. Huang, W. Tang, and Q. Wu, "Resilient economic control for distributed microgrids under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4435–4446, 2021.

[2] P. S. Tadepalli, M. N. Alam, and D. Pullaguram, "Cyber resilient fully distributed secondary control for inverter dominant AC microgrid," in *Proc. Int. Conf. Power Electron. Converters for Transportation and Energy Applications (PECTEA)*, pp. 1–6, 2025.

[3] H. Shafei, M. Farhangi, L. Li, R. P. Aguilera, and H. H. Alhelou, "A novel cyber-attack detection and mitigation for coupled power and information networks in microgrids using distributed sliding mode unknown input observer," *IEEE Trans. Smart Grid*, vol. 16, no. 2, pp. 1667–1681, 2024.

[4] S. M. Mohiuddin and J. Qi, "Attack resilient distributed control for AC microgrids with distributed robust state estimation," in *Proc. IEEE Texas Power and Energy Conf. (TPEC)*, pp. 1–6, 2021.

[5] Y. Wang, C. Deng, Y. Liu, and Z. Wei, "A cyber-resilient control approach for islanded microgrids under hybrid attacks," *Int. J. Electr. Power Energy Syst.*, vol. 147, p. 108889, 2023.

[6] F. Zargarzadeh-Esfahani, B. Fani, B. Keyvani-Boroujeni, I. Sadeghkhani, and M. Sajadieh, "Resilient oscillator-based cyberattack detection for distributed secondary control of inverter-interfaced islanded microgrids," *Scientific Reports*, vol. 15, no. 1, p. 20685, 2025.

[7] A. G. Miles, Y. Chakhchoukh, and S. M. S. Alam, "Robust distribution state estimation for reliable locational marginal pricing under cyber-attacks," *IEEE Transactions on Power Systems*, vol. 39, no. 3, pp. 4963–4974, 2023.

[8] M. Rashed, I. Gondal, J. Kamruzzuman, and S. Islam, "State estimation in the presence of cyber attacks using distributed partition technique," in *Proc. Australasian Universities Power Engineering Conf. (AUPEC)*, 2020, pp. 1–6.

[9] M. Göl and A. Abur, "A modified Chi-Squares test for improved bad data detection," in *Proc. IEEE Eindhoven PowerTech*, 2015, pp. 1–5.

[10] A. K. M. A. Habib, M. K. Hasan, A. Alkhayyat, S. Islam, R. Sharma, and L. M. Alkwai, "False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction," *Computers and Electrical Engineering*,

vol. 107, Art. no. 108638, 2023.

[11] X. Li, Y. Wang, and Z. Lu, "Graph-based detection for false data injection attacks in power grid," *Energy*, vol. 263, Art. no. 125865, 2023.

[12] Y. Wang, A. Xing, Z. Qu, X. Han, H. Dong, and M. G. Popov, "False data injection attack detection based on interval affine state estimation," *Electric Power Systems Research*, vol. 210, Art. no. 108100, 2022.

[13] A. Malhotra, S. Yadav, R. Jain, and R. Yadav, "Multi-objective optimization of cyber-topology attacks in power systems," in *Proc. IEEE 4th Int. Conf. Sustainable Energy and Future Electric Transportation (SEFET)*, 2024, pp. 1–6.

[14] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, Art. no. 108975, 2023.

[15] X. Yang, Z. Hu, R. Fan, H. Xu, H. Yang, Y. Wang, and X. Tian, "Weighted least squares state estimation based on the optimal weight," in *Proc. Int. Conf. Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*, 2015, pp. 12–16.

[16] M. E. Baran and A. W. Kelley, "State estimation for real-time monitoring of distribution systems," *IEEE Transactions on Power Systems*, vol. 9, no. 3, pp. 1601–1609, 2002.

[17] A. Alamin, H. M. Khalid, and J. C.-H. Peng, "Power system state estimation based on iterative extended Kalman filtering and bad data detection using normalized residual test," in *Proc. IEEE Power and Energy Conf. at Illinois (PECI)*, 2015, pp. 1–5.

[18] T. P. Vishnu, V. Viswan, and A. M. Vipin, "Power system state estimation and bad data analysis using weighted least square method," in *Proc. Int. Conf. Power, Instrumentation, Control and Computing (PICC)*, 2015, pp. 1–5.

[19] A. Malhotra, S. Singh, and R. Yadav, "Modelling and distinction of cascade tripping attacks in power system," in *Proc. Second Int. Conf. Smart Technologies for Smart Nation (SmartTechCon)*, 2023, pp. 765–769.

[20] H. Wu, X. Huang, L. Li, and Z. Wu, "Observability analysis and state estimation of distribution network," in *Proc. IEEE Conf. on Energy Internet and Energy System Integration (EI2)*, 2023, pp. 246–252.

[21] J. Olowolaju and H. Livani, "Enhanced power system state estimation using grid aware learning method," in *Proc. IEEE Kansas Power and Energy Conf. (KPEC)*, 2025, pp. 1–5.

[22] B. L. H. Nguyen, T. V. Vu, T. H. Ortmeyer, and T. Ngo, "Distributed dynamic state estimation for microgrids," in *Proc. IEEE Power & Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.

[23] M. Pau and P. A. Pegoraro, "WLS-based state estimation for unobservable distribution grids through allocation factors evaluation," *IEEE Transactions on Instrumentation and Measurement*, vol. 73, pp. 1–13, 2024.

[24] A. Malhotra, B. Sharma, and R. Yadav, "Impact assessment of topology attack on power system using graph theory," in *Proc. IEEE Int. Conf. Power and Energy (PECon)*, 2024, pp. 98–103.

[25] A. Shahbazian and T. Amraee, "Automatic bad data detection in state estimation using an optimization model," in *Proc. Int. Electrical Power Distribution Conf. (EPDC)*, 2024, pp. 1–3.

[26] M. A. Majeed, N. K. Singh, L. Tak, and V. Mahajan, "Detection of stealthy cyber intrusion in smart electric grid using advanced state estimation," in *Proc. Int. Conf. Cloud Computing, Data Science & Engineering (Confluence)*, 2021, pp. 660–665.

[27] Y. Han and S. Li, "Detection of bad data and cyber attacks in state estimation using support vector machine," in *Proc. IEEE PES Innovative Smart Grid Technologies–Asia (ISGT Asia)*, 2022, pp. 111–115

Algorithm 1 Nonlinear Weighted Least Squares (WLS) State Estimation

Require: Measurement vector $z \in \mathbb{R}^m$; measurement covariance matrix $R \in \mathbb{R}^{m \times m}$; initial state estimate $x_0 \in \mathbb{R}^n$; network topology and parameters $\mathcal{M}, \mathcal{S}, \mathcal{G}$; convergence tolerance ϵ_{tol}; maximum iterations $k_{\max}$

Ensure: Estimated state vector x; residual covariance matrix S; residual vector r; convergence flag *converged*

$x \leftarrow x_0$
$k \leftarrow 0$
converged $\leftarrow$ **false**
$W \leftarrow R^{-1}$ ▷ Weight matrix
while $k < k_{\max}$ **and not** *converged* **do**
    $(V, \delta) \leftarrow \textsc{StateVectorToDicts}(x, \mathcal{S})$
    $h(x) \leftarrow \textsc{CalculateMeasurementVector}(\mathcal{M}, V, \delta, \mathcal{G})$
    $r \leftarrow z - h(x)$
    $H \leftarrow \textsc{ComputeJacobian}(\mathcal{M}, \mathcal{S}, V, \delta, \mathcal{G})$
    $G \leftarrow H^T W H$ ▷ Gain matrix
    if $\text{rank}(G) < n$ **then**
        return x, **null**, r, **false** ▷ System unobservable
    end if
    Solve $G\Delta x = H^T W r$
    $x \leftarrow x + \Delta x$
    if $\|\Delta x\|_2 < \epsilon_{\text{tol}}$ **then**
        converged $\leftarrow$ **true**
    end if
    $k \leftarrow k + 1$
end while
if *converged* **then**
    $(V, \delta) \leftarrow \textsc{StateVectorToDicts}(x, \mathcal{S})$
    $h(x) \leftarrow \textsc{CalculateMeasurementVector}(\mathcal{M}, V, \delta, \mathcal{G})$
    $r \leftarrow z - h(x)$ ▷ Final residuals
    $H \leftarrow \textsc{ComputeJacobian}(\mathcal{M}, \mathcal{S}, V, \delta, \mathcal{G})$ ▷ Update Jacobian at solution
    $G \leftarrow H^T W H$ ▷ Update Gain matrix
    $G^{-1} \leftarrow \textsc{Inverse}(G)$
    $S \leftarrow R - H G^{-1} H^T$ ▷ Residual covariance matrix
    return x, S, r, **true**
else
    return x, **null**, r, **false**
end if