Voting-Based Hybrid Framework for Robust Anomaly Detection in Smart Grid Communication Networks

Sharon A. Boamah[1] Priya Mittal[1] Michel Caraballo[2] Janise McNair[1] Arturo Bretas[2,3]
[1]Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA
[2]Univ. Grenoble Alpes, CNRS, Grenoble INP*, G2Elab, 38000 Grenoble, France
[3]Grid Security and Communications Department, Sandia National Laboratories, Albuquerque, NM, USA
{sharonboamah, mittal.priya}@ufl.edu, michel.caraballo-gomez@grenoble-inp.fr, mcnair@ece.ufl.edu, asbreta@sandia.gov

***Abstract*—The reliability and robustness of the communication network are critical to ensure that the smart grid operates seamlessly with little to no interruptions. Cyber-attacks like False Data Injections compromise packets in the communication network, making the smart grid vulnerable. Hence, it is important to ensure data integrity and reliability of the network. In this work, we present and implement a weighted-voting hybrid framework that combines network physics-informed models (conventional and extended) with IsoForest-LSTM (Isolation Forest plus LSTM). The extended network physics-informed model enhances detection of previously masked gross errors by achieving 70% recall, more than twice that of the conventional model. IsoForest-LSTM captures subtle anomalies to improve recall by 90%. Combining decisions from these models and applying weighted voting, the proposed hybrid framework achieves a near-perfect performance by significantly improving recall and F_1-score compared to the standalone models. Hence, the experimental results validate the effectiveness of the hybrid framework to provide reliable decisions in securing the communication network.**

***Index Terms*—cyber-attacks, reliability, weighted-voting, communication network, smart grid, hybrid framework**

I. Introduction

Modern network technologies have significantly contributed to the realization of the smart grid, which comprises grid components, sensors, and communication network devices for real-time data transmission. The increasing interconnection and digitalization of modern power systems have expanded the attack surface of smart grids. Power outages from vulnerabilities in the smart grid are estimated to cost the United States $80 billion annually [1]. This can serve as a motivation for terrorism-based cyber-attacks. Hence, anomaly detection to assess the state of the communication network is a critical component of smart grid reliability.

Previous works in [2], [3] have shown that Machine Learning (ML) methods like Isolation Forest (IF), AutoEncoders (AE), and Support Vector Machines can spot irregularities in sensor data, but they treat the grid as a black box and ignore its physics. Likewise, a study in [4] on class imbalance for intrusion detection did not exploit measurement redundancy or observability to improve accuracy. Studies in [5] improve residual-based detection in [1], [6] by introducing Composed Measurement Error (CME) that combines detectable and undetectable errors for robustness. However, the standalone models in [1]–[4], [6], while effective in capturing anomalies, are limited by model and data dependencies.

Support is gratefully acknowledged from the U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (DOE-CESER).

Recent research has introduced ensemble methods that combine multiple models for more reliable anomaly detection. The authors in [7] present Ensemble CorrDet with Adaptive Statistics (ECD-AS), which aggregates multiple CorrDet detectors and demonstrates improved performance by learning statistical features from grid and communication networks. However, [8] questions the robustness of ECD-AS to stealthy False Data Injection (FDI) attacks, presenting that intruders aware of these statistics can craft undetectable FDIs. They propose an encryption framework to modify measurement statistics and enhance detection. But since ECD-AS detectors use the same logic, they share the same biases, limiting improvements in decision reliability.

The need for a more reliable anomaly detection has driven research toward hybrid frameworks combining heterogeneous models. In [9], a hybrid statistical-ML model was presented that uses the Seasonal Autoregressive Integration Moving Average and Long Short-Term Memory (LSTM) to detect anomalies in industrial cyber-physical network traffic (i.e., packet and arrival time distributions). While effective for forecasting-based detection, it neglects the system's underlying physics in decision-making. Studies in [10] and [11] integrate ECD-AS with physics-informed models for improved anomaly detection in [7], but their fusion method suffers when one model underperforms. Research in [11] ignores undetectable errors, making the communication network vulnerable, while [10] addresses this with CME only for the power grid, not the communication network.

Overall, prior works apply ML or physics-informed models, and some use ensemble and hybrid methods, but rarely tackle the communication network layer, where data integrity and latency are critical. Also, others ignore CME that enhance robustness. These gaps motivate our research in this unexplored area, where we combine the extended Network Physics-Informed (NPI) and ML models through a weighted-voting scheme for reliable anomaly detection in the communication network.

The contributions of this work to the state-of-the-art are outlined as follows.

- Formulate a normalization strategy to standardize network statistics for robustness against scaling inconsistencies and poor conditioning from measurement variability across heterogeneous communication channels.
- Design an application of the extended Network Physics-Informed model for FDI detection in communication networks by integrating detectable and undetectable error components in the measurement model.

979-8-3315-8138-1

- Implement an IsoForest-LSTM model useful for forecasting time series data for FDI anomaly detection.
- Develop a novel weighted-voting hybrid framework, combining extended and conventional NPIs with IsoForest-LSTM models for reliable FDI detection.

The remaining sections of the paper are organized as follows. Section II provides the background information on the baseline models relevant to this study. Section III describes the proposed hybrid framework for detecting anomalies. Section IV presents a case study and discusses the research findings. Section V summarizes the findings of the work.

II. Background Information

A. Measurement Error Detection: From Conventional to Extended Network Physics-Informed Models

Detecting Gross Error (GE) in measurement data requires distinguishing between detectable (e_D) and undetectable errors (e_U). Detectable errors affect measurement residuals and can be identified through statistical tests, whereas Undetectable errors remain hidden within the estimation process.

State estimation minimizes the weighted squared residuals between measurements z and predicted values $h(x)$, as in (1).

$$\hat{x} = \arg\min_{x} \; J(x), \quad J(x) = \sum_{i=1}^{m} (z_i - h_i(x))^2 \Omega_{ii}^{-1} \tag{1}$$

where $z \in \mathbb{R}^m$ is the measurement vector, $x \in \mathbb{R}^N$ is the state vector, $h(x) : \mathbb{R}^N \to \mathbb{R}^m$ is the nonlinear measurement function, and Ω is the residual covariance, $E[rr^T] = (I - P)cov(e)$, with mean $E(e) = (I - P)E(e) = 0$. The measurement error e is assumed Gaussian with zero mean and standard deviation σ. Measurements are normalized by their maximum values for consistent scaling and proper numerical conditioning across heterogeneous units and magnitudes. The normalized measurement vector represents the observed communication-layer parameters: Inter-Arrival Time (IAT), Transmission Delay (TD), Packet Count (PC), and Roundtrip Time (RTT), defined in (2).

$$z = \begin{cases} IAT_{norm} = \frac{IAT}{max(IAT)} \\ TD_{norm} = \frac{TD}{max(TD)} \\ PC_{norm} = \frac{PC}{max(PC)} \\ RTT_{norm} = \frac{RTT}{max(RTT)} \end{cases} \tag{2}$$

The network state vector, $\mathbf{x}$ from the normalized network measurements, is given in 3, where λ_{norm} and μ_{norm} are the normalized arrival and service rates, respectively.

$$\mathbf{x} = \begin{bmatrix} \lambda_{norm} = \frac{1}{IAT} \times min(IAT) \\ \mu_{norm} = \left(\frac{1}{TD} + \frac{1}{IAT}\right) \times \min(TD + IAT) \end{bmatrix} \tag{3}$$

The mapping from state to measurements follows queueing theory, which describes how observable metrics depend on the underlying arrival and service rates, as shown in (4).

$$\mathbf{z} = \begin{bmatrix} IAT_{norm} \\ TD_{norm} \\ PC_{norm} \\ RTT_{norm} \end{bmatrix} = \mathbf{h}(\mathbf{x}) + \mathbf{e} = \begin{bmatrix} \frac{1}{\lambda_{norm}} \\ \frac{1}{\mu_{norm} - \lambda_{norm}} \\ \lambda_{norm} W \\ \alpha + \frac{1}{\mu_{norm}} + W_q \end{bmatrix} + \mathbf{e} \tag{4}$$

Similar to [11], the mean waiting time is $W = 1/\mu_{norm} + W_q$, with queueing delay $W_q = 1/(\mu_{norm} - \lambda_{norm})$, and propagation delay is $\alpha = d/s$, where d is transmission distance and s link speed.

The measurement space $\mathbb{R}^m$ can be decomposed into detectable and undetectable errors [12]. Mathematically, the space decomposes into the range of the Jacobian, $\Re(H)$, containing undetectable errors e_U, and its orthogonal complement, $\Re(H)^\perp$, containing detectable errors e_D:

$$\mathbb{R}^m = \Re(H) \oplus \Re(H)^\perp, \quad e = e_U + e_D \tag{5}$$

Residuals depend only on e_D, so a small residual does not guarantee accurate estimation. The weighted error norm separates as:

$$\|e\|_{R^{-1}}^2 = \|e_U\|_{R^{-1}}^2 + \|e_D\|_{R^{-1}}^2 \tag{6}$$

The Innovation Index (II) links detectable and undetectable components [13]:

$$II_i = \frac{\|e_D^i\|_{R^{-1}}}{\|e_U^i\|_{R^{-1}}} = \frac{\sqrt{1 - P_{ii}}}{\sqrt{P_{ii}}} \tag{7}$$

where P is the projection matrix.

The CME captures the total error magnitude :

$$\text{CME}_i^2 = e_{U_i}^2 + e_{D_i}^2 = \left(1 + \frac{1}{II_i^2}\right) e_{D_i}^2 \tag{8}$$

Incorporating the CME into a chi-square test extends gross error detection from the conventional residual space $\mathbb{R}^{m-N}$ to the full measurement space $\mathbb{R}^m$:

$$\hat{x} = \arg\min_{x} \; J_C(\hat{x})$$
$$\text{s.t. } J_C(\hat{x}) = \sum_{i=1}^{m} \left(\frac{CME_i}{\sigma_i}\right)^2, \; \begin{cases} J_C(\hat{x}) > \chi_{m,\gamma}^2 & \text{(GE)}, \\ J_C(\hat{x}) \le \chi_{m,\gamma}^2 & \text{(No GE)}. \end{cases} \tag{9}$$

where γ is the confidence level of the test, e.g., 98%.

Since direct computation is costly, [12] introduced an II-based formulation that implicitly represents the undetectable subspace and extends the estimation space to $\mathbb{R}^m$. The processing steps are summarized in Algorithm 1, applied here to the communication layer.

Algorithm 1 Processing a New Data Set [12]

1) **Normalization:** Normalize all measurements to system base values.
2) **Covariance estimation:** Assume any measurement may contain a GE and set its standard deviation as a small fraction of the nominal value to get R.
3) **State estimation:** Using normalized measurements z, measurement model $h(x)$, and an initial flat start of x, minimize the cost function in (9).
4) **Gross error detection:** After convergence (or iteration limit), apply the chi-square test in (9) to detect GE.

B. IsoForest-LSTM

The IsoForest–LSTM framework referred to in this work integrates LSTM Autoencoder and Isolation Forest models, leveraging their complementary strengths, which are temporal feature learning and structural outlier detection, respectively.

1) LSTM Autoencoder: It is designed to capture temporal dependencies and reconstruct normal behavior patterns from multivariate time-series data.

- Encoder: Two stacked LSTM layers ($128 \rightarrow 48$ units) compress 200×7 input sequences to low-dimensional latent representations, with dropout (0.1) and layer normalization to curb overfitting and stabilize features.
- Decoder: The latent vector is repeated across time-steps and passed through symmetric LSTM layers to reconstruct the input, with Mean Squared Error quantifying reconstruction accuracy for normal data.
- Anomaly Score (AE_{topk}): The AE anomaly score is the mean of the top 10% reconstruction errors per sample, capturing local deviations indicative of anomalies.

2) Isolation Forest on Latent Space: The encoder's latent outputs train an IF that isolates anomalies through random feature space partitioning. Anomalies require fewer splits than normal samples, producing scores inversely related to normality, which are min-max normalized to $[0, 1]$.

3) IsoForest-LSTM (AE $\times$ IF): To utilize both reconstruction-based and structure-based information, a weighted hybrid score is computed:

$$S_{\text{IF-LSTM}} = w \cdot S_{\text{AE}_{topk}} + (1 - w) \cdot S_{\text{IF}} \tag{10}$$

The weight w, optimized via grid search to maximize F_2 score, determines the AE's contribution and balances temporal error sensitivity with IF's structural outlier detection.

4) Threshold Optimization: The threshold τ is optimized by sweeping quantiles $(0.500–0.999)$ to maximize F_2-score, prioritizing recall. The selected optimal value $\tau = 0.951$ balances precision and recall.

III. Weighted-Voting Hybrid Framework for Anomaly Detection

To the best of our knowledge, this is the first study to provide a unified framework that combines network physics-informed models with the IsoForest-LSTM model and applies weighted voting for more reliability in anomaly detection. Hence, this section discusses the novel weighted-voting hybrid framework introduced in this work for detecting anomalies in the communication network of the smart grid. Fig. 1 shows the workflow of the proposed hybrid anomaly detection framework that utilizes the weighted-voting scheme. The hybrid framework combines NPI models with machine learning models to complement each other's strengths. As discussed in Sections II-A and II-B, the NPI models capture interpretable unexpected behavior using the deviations from residuals, while the IsoForest-LSTM model captures subtle anomalies in temporal data patterns. Weighted voting, as proven in [14] has demonstrated more effectiveness in providing reliable decisions to detect anomalies than the majority rule voting method. It is considered in this work, especially when these models have unequal performances.

In the weighted-voting scheme, each model is assigned a weight, w_i, based on its classification performance on samples. The weighted scores are aggregated to obtain a final score, S_{hyb}. The final decision, D_{hyb} on normal or anomalous samples, is obtained by thresholding the sum of the weighted scores, which is the class with the highest votes. This ensures that under-performing models have less influence in the final decision, whereas high-performing models strongly impact

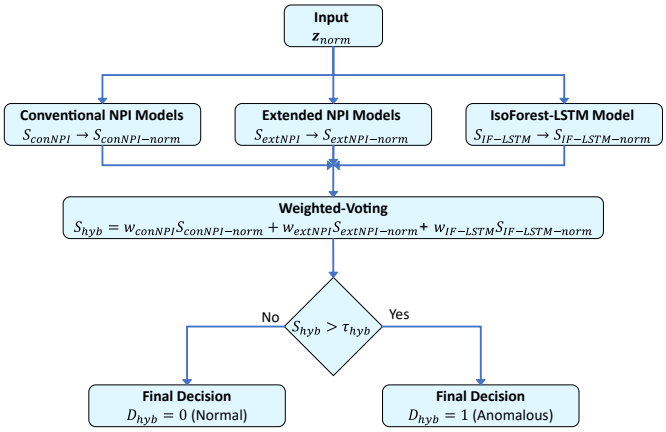

Fig. 1: Overall Flowchart of the Proposed Weighted-Voting Hybrid Framework for Detecting Anomalies

the final decision for classification. The process for the weighted-voting is mathematically modeled in (11).

$$\begin{aligned} D_{\text{hyb}} &= \begin{cases} 1, & \text{if } S_{\text{hyb}} > \tau_{\text{hyb}} \\ 0, & \text{otherwise} \end{cases} \\ S_{\text{hyb}} &= \sum_{i=1}^{K} w_i \, S_i \\ \text{s.t.} \quad w_i &\geq 0, \quad \sum_{i=1}^{K} w_i = 1 \end{aligned} \tag{11}$$

Where K is the total number of models, and $i = 1, 2, \ldots, K$ indexes each model. The weight w_i assigned to the ith model is constrained to be positive and normalized to sum up to 1. The decision threshold is denoted as τ_{hyb} and is used to determine whether the final decision on a sample is anomalous (1) or normal (0).

IV. Case Study Implementation

The framework is tested on a 14-bus network architecture as in [11]. To emulate a realistic communication network behavior, we utilize SimPy, which is an open-source discrete event simulator, to generate the network parameters: IAT, TD, PC, and RTT considered in this work. These normalized network measurements represent the temporal and statistical behavior of packets in the communication network under normal and anomalous cases. The dataset consists of $200,000$ network measurements embedded with Gaussian noise, spread across 250 samples, where each sample has 200 measurements for each of the four defined measurement types. The Gaussian noise added to the measurements for uncertainties has zero mean and a standard deviation of 0.5%.

The FDI implementation involves compromising a single measurement from 4% of the total samples consecutively to evaluate the sensitivity of these models in detecting bad data. The size of the FDI attack is generated as a zero-mean Gaussian noise with a standard deviation proportional to the measurement magnitude scaled by $8\% \pm 0.01$, sampled from a Gaussian distribution. This allows the injected FDI to vary slightly across different measurement samples. The size of the state vector is 28, resulting in a Global Redundancy Level ($GRL = m/N$) of 7.14. For the conventional NPI, the Chi-square threshold is 854.828 (normalized value is 0.992), corresponding to 772 degrees of freedom ($m - N$)

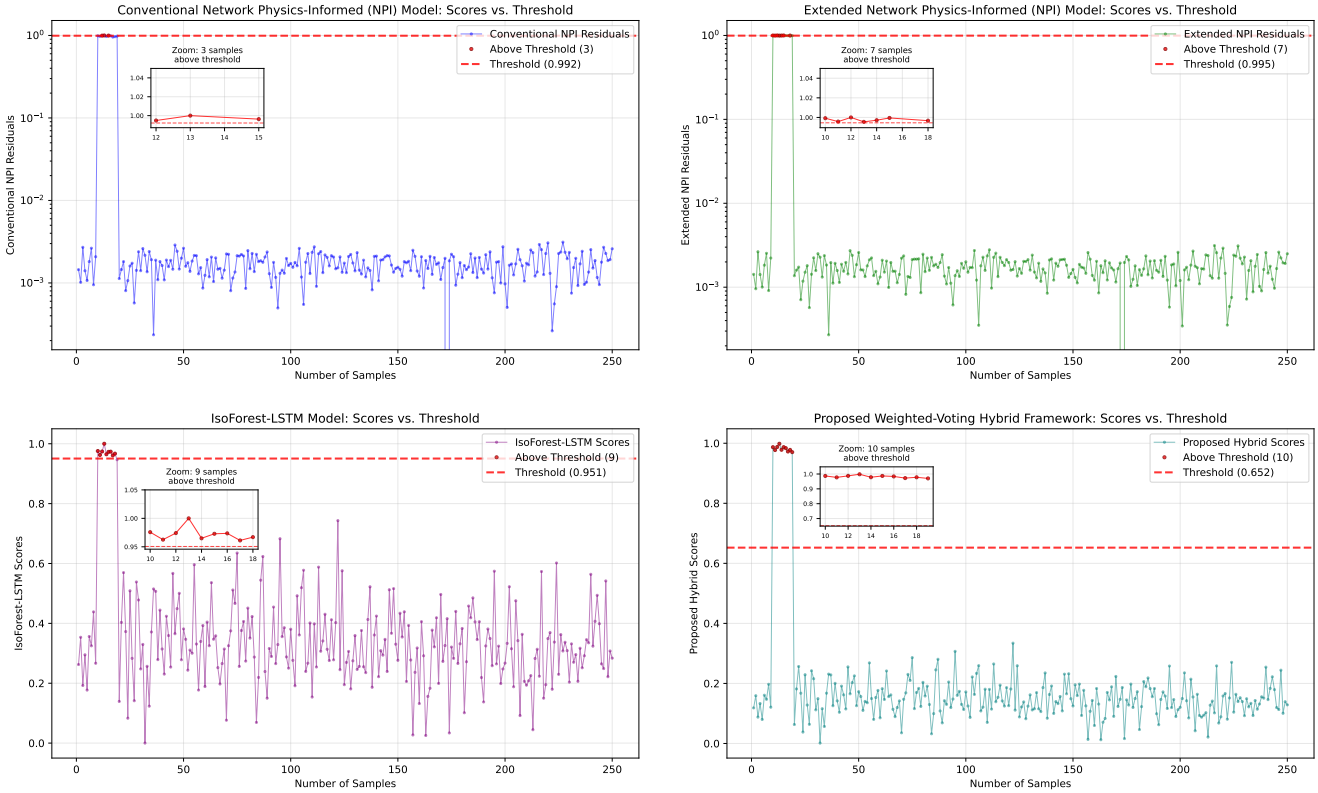

Fig. 2: False Data Injection Attack Detection Comparison Across the Models

at 98% confidence level. The extended NPI has a Chi-square threshold of 884.279 (normalized value of 0.995) with 800 degrees of freedom (m) at 98% confidence level.

LSTM AE trained on normal data captures temporal patterns, while IF detects structural anomalies in latent space. Their weighted fusion yields the IsoForest-LSTM anomaly score. The fusion weight (w) and threshold (τ) were optimized through grid search and F_2-score maximization, respectively, emphasizing recall for reliable anomaly detection.

Parameter Discussion: Several parameters in the IsoForest-LSTM framework significantly influenced performance:

- **Latent Dimension (48):** A 48-dimensional latent space was chosen to balance temporal features with model generalization, avoiding underfitting from small values and high reconstruction variance from large values.
- **Top-k Fraction (10%):** AE anomaly scores used the top 10% reconstruction errors per sample, amplifying sensitivity to short-term deviations.
- **Fusion Weight (w):** Reducing the AE weight emphasized IF's structural anomaly detection, enhancing recall without significantly compromising precision.
- **Threshold (τ):** Optimized F_2 thresholds prioritize recall to capture subtle anomalies, improving precision-recall balance over fixed cutoffs.

The weighted-voting hybrid framework assigns weights ($0.175, 0.375$, and 0.448) based on the F_2-score performance of each of the three models (conventional NPI, extended NPI, and IsoForest-LSTM). The threshold, τ_{hyb}, is set as 0.652 using the midpoint method, which has been proven to effectively classify slightly distinguishable data distributions.

A. Results and Analysis

The performance of the proposed weighted-voting hybrid framework is compared with conventional NPI, extended NPI, and IsoForest-LSTM. Figure 2 illustrates the residuals and decision scores obtained from the presented hybrid model and the three baseline models (conventional NPI, extended NPI, and IsoForest-LSTM) against their thresholds. The models classify samples as anomalous when their residuals or decision scores exceed the threshold value, indicated as a red line. Samples with residuals or decision scores below the red threshold line are detected as normal. The conventional and extended NPIs show high sensitivity to large-magnitude FDIs, assigning high penalties to these errors from the models. This results in large residuals for anomalous samples and small residuals for normal samples, depicting a separation between the anomalous and normal samples. The extended NPI detects more large-magnitude FDI than the conventional NPI from its inclusion of previously undetectable errors. However, both NPIs assign low residuals to subtle FDI and fail to detect them. The IsoForest-LSTM learns temporal patterns to detect the subtle FDIs improving on the number of detected anomalous samples. The proposed hybrid framework integrates insights from the baseline models to provide superior performance in distinguishing normal and anomalous samples.

We evaluate these models using precision, recall, F_1-Score, accuracy, and confusion matrix (true negative (TN), false positive (FP), false negative (FN), true positive (TP)) metrics. Table I summarizes the performance outcome for these models. All models generally demonstrate high precision and accuracy in detecting normal samples. The NPIs correctly classify normal samples with high TNs but miss anomalies with low recall (from low TP) and F_1-score (from low TP and high FP). The extended NPI improves the anomalous class performance of the conventional NPI (with TP$=3$) by detecting more than twice as many anomalies (with TP$=7$),

TABLE I: Performance of Models for Bad Data Detection

Model	Class	Prec.	Rec.	F1	Acc.	TN	FP	FN	TP
Conv. NPI	Normal	0.970	1.000	0.990	0.972	240	7	0	3
	Anomalous	1.000	0.300	0.460					
Ext. NPI	Normal	0.990	1.000	0.990	0.988	240	3	0	7
	Anomalous	1.000	0.700	0.820					
IsoForest-LSTM	Normal	0.996	1.000	0.998	0.996	240	1	0	9
	Anomalous	1.000	0.900	0.947					
Proposed Hybrid	Normal	1.000	1.000	1.000	1.000	240	0	0	10
	Anomalous	1.000	1.000	1.000					

resulting in a recall from 30% to 70% and an F_1-score from 46% to 82%. It achieves this by incorporating previously undetectable errors in the detection process. However, it still misclassifies three anomalous samples due to its limited ability to detect subtle FDI attacks.

The IsoForest-LSTM outperforms the NPIs by resolving their limitation using temporal patterns and scoring to improve the detection of subtle FDI attacks. Out of the 250 total samples, only one was misclassified (a high-magnitude FDI), resulting in an overall accuracy of 99.6%. For the anomalous class, the model achieved a precision of 100%, a recall of 90%, and an F_1-score of 94.74%. These results indicate that IsoForest-LSTM effectively combined the LSTM's reconstruction-based detection with the IF's structure-based scoring. The adaptive threshold selection and weighting improved recall while maintaining high precision, demonstrating the model's robustness in identifying temporal and distributional anomalies compared to the NPIs.

The hybrid framework achieved the highest performance. It leverages the complementary strengths of the NPIs and IsoForest-LSTM with weighted voting to provide more reliable decisions for detecting anomalies. It maintains a high accuracy (from high TN), precision (from high TP and low FP), recall (from high TP), and F_1-score (from high TP and low FP) of 100%. While the NPIs demonstrated reliable detection of normal samples and the IsoForest-LSTM effectively identified subtle FDIs, the hybrid model achieved near-perfect discrimination between normal and anomalous samples. This result validates the effectiveness of the proposed framework.

V. Conclusion

This paper presents a novel hybrid framework with weighted-voting to improve robustness in detecting FDI attacks at the communication network layer of the smart grid. The proposed framework integrates the physics-informed models (conventional and extended), which perform residual-based Chi-square analysis with IsoForest-LSTM (combined IF and LSTM), which leverages temporal pattern and decision scoring for reliable anomaly detection. The weighted voting scheme is applied for high-performing models to have a stronger influence on the final decision. A case study is presented to test the hybrid framework on a 14-bus network architecture. The results show that the extended NPI improves detecting gross error by over twice that of the conventional NPI but misses subtle FDIs. The IsoForest-LSTM demonstrates its ability in detecting subtle FDIs to improve recall. When these models were combined, the proposed hybrid framework achieved near-perfect classification, validating its effectiveness and offering a promising direction for reliability and robustness of the communication network.

Acknowledgement

The authors acknowledge UFIT Research Computing for providing computational resources and support that have contributed to the research results reported in this publication. URL: http://www.rc.ufl.edu. The authors thank the U.S. Department of Energy (DoE), Office of Cybersecurity, Energy Security, and Emergency Response (DOE-CESER), and Sandia National Laboratories for the funding of this research. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the document do not necessarily represent the views of the U.S. Department of Energy or the U.S. Government.

References

[1] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[2] E. Omol, L. Mburu, and D. Onyango, "Anomaly detection in iot sensor data using machine learning techniques for predictive maintenance in smart grids," *International Journal of Science, Technology & Management*, vol. 5, no. 1, pp. 201–210, 2024.

[3] P. K. R. Shabad, A. Alrashide, and O. Mohammed, "Anomaly detection in smart grids using machine learning," in *IECON 2021–47th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2021, pp. 1–8.

[4] C. Promper, D. Engel, and R. C. Green, "Anomaly detection in smart grids with imbalanced data methods," in *2017 IEEE symposium series on computational intelligence (SSCI)*. IEEE, 2017, pp. 1–8.

[5] N. G. Bretas and A. S. Bretas, "The extension of the gauss approach for the solution of an overdetermined set of algebraic non linear equations," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 9, pp. 1269–1273, 2018.

[6] A. Cooper, A. Bretas, and S. Meyn, "Anomaly detection in power system state estimation: Review and new directions," *Energies*, vol. 16, no. 18, p. 6678, 2023.

[7] A. Starke, K. Nagaraj, C. Ruben, N. Aljohani, S. Zou, A. Bretas, J. McNair, and A. Zare, "Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security," *IET Smart Grid*, vol. 5, no. 6, pp. 398–416, 2022.

[8] K. Nagaraj, N. Aljohani, S. Zou, T. Zou, A. S. Bretas, J. McNair, and A. Zare, "Smart fdi attack design and detection with data transmutation framework for smart grids," in *2021 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2021, pp. 1–5.

[9] W. Hao, T. Yang, and Q. Yang, "Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems," *IEEE Transactions on Automation Science and Engineering*, vol. 20, no. 1, pp. 32–46, 2021.

[10] C. Ruben, S. Dhulipala, K. Nagaraj, S. Zou, A. Starke, A. Bretas, A. Zare, and J. McNair, "Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security," *IET Smart Grid*, vol. 3, no. 4, pp. 445–453, 2020.

[11] S. A. Boamah, R. Mathieu, V. Faillace, D. Agnew, J. McNair, and A. Bretas, "Data fusion-based hybrid framework for cyber-physical security of the smart grid," in *2024 Resilience Week (RWS)*. IEEE, 2024, pp. 1–8.

[12] A. S. Bretas, N. G. Bretas, J. B. London, and B. E. Carvalho, "Chapter 7 - the innovation methodology for error analysis in power systems," in *Cyber-Physical Power Systems State Estimation*, A. S. Bretas, N. G. Bretas, J. B. London, and B. E. Carvalho, Eds. Elsevier, 2021, pp. 183–210. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780323900331000068

[13] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210–219, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779617301657

[14] A. Dogan and D. Birant, "A weighted majority voting ensemble approach for classification," in *2019 4th international conference on computer science and engineering (UBMK)*. IEEE, 2019, pp. 1–6.