Data Fusion-based Hybrid Framework for Cyber-Physical Security of the Smart Grid

Sharon A Boamah, Reynold Mathieu, Victor Faillace, Dennis Agnew, Janise Mcnair, Arturo Bretas

Data Fusion-based Hybrid Framework for Cyber-Physical Security of the Smart Grid

Sharon A. Boamah[1] Reynold Mathieu[1] Victor Faillace[1] Dennis Agnew[1] Janise McNair[1] Arturo Bretas[1,2,3]
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL [1]
Electric Grid Security and Communications Department, Sandia National Laboratory, Albuquerque, NM [2]
G2Elab, Grenoble INP, CNRS, Université Grenoble Alpes, 38000 Grenoble, France [3]
{sharonboamah, reynold.mathieu, vfaillace, dennisagnew}@ufl.edu, {mcnair, arturo}@ece.ufl.edu

***Abstract*—The integration of information communication technology with the power grid exposes it to cyber threats. The state estimation process provides stability to the smart grid. The communication network plays a major role in ensuring the successful transmission of state information. However, these network measurements are vulnerable to malicious attacks. This subsequently affects the network measurement such as associated high transmission delays and packet losses affecting the reliability of the smart grid. In this work, we propose a hybrid physics-based data-driven model that uses data fusion from the state-of-the-art physics-based Network State Estimation model and a data-driven model to detect false data injection attacks in the communication network layer of the smart grid. The performance of the data fusion method is evaluated and the simulation results show that the proposed model outperforms the standalone approaches in the detection of bad data. This shows that the proposed scheme is able to improve the cyber-physical security of the communication network layer of the smart grid.**

***Index Terms*—cyber-physical security, smart grid, state estimation, false data injection, communication network**

I. Introduction

To provide a more efficient and dependable grid, the conventional power grid has evolved through technological advancements, leading to the adoption and prevalence of the smart grid. Unlike the traditional power grid with a one-way power flow, the smart grid utilizes a bidirectional flow of power in the grid layer and data in the communication network layer. This has demonstrated the potential of the modern grid in different aspects of its operations including efficiency and automation in monitoring and control [1]. The smart grid leverages Information and Communication Technologies (ICTs) to send instantaneous reports on the status of the power grid to remote control facilities such as the Supervisory Control and Data Acquisition (SCADA) system [2]. The power grids mostly span across large geographical areas and are connected to the control system through communication networks such as Wide Area Networks (WANs) [3]. The smart grid is thereby regarded as a cyber-physical system since it integrates control, computation, and communication [4].

Despite the benefits associated with the smart grid, the reliance of the power grid on the communication network increases its attack surface making it susceptible to cyber-attacks. As the power system is typically far away from the control center, it becomes vulnerable to attacks that can target the power grid, control center, or communication network. The newly introduced cyber-related issues in the smart grid were non-existent in the traditional power grid. Several cyber-attacks have proven successful in disrupting the normal operations of the smart grid, and historical evidence is the major Ukraine blackout in 2015 [5]. It is of critical importance to ensure the confidentiality, integrity, and availability of the smart grid through guaranteed cyber-physical security. Numerous research efforts and contributions have been directed toward addressing the security challenges in the smart grid to ensure its reliable operation.

State Estimation (SE) plays a major role in securing the control and monitoring of the smart grid through its ability to correct errors, hence its wide adoption in the power grid [4]. SE determines the current status of the power grid by using remotely captured measurements and topology information from SCADA for reactive control actions [6]. However, the state estimation process faces vulnerabilities since the measurements used for predicting the condition of the smart grid can be corrupted. This can cause the state estimator to make erroneous decisions.

Current research works are focused on efficient approaches to estimate the state of the power grid [5], [7]–[11], while the cyber-physical security of the communication network of the smart grid is still developing. Our previous research considers a cross-layered framework [12], [13]. In this framework, we employ SE, which uses only power grid data, as well as a machine learning model, Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS), which combines data from both the power and historical data from the communication network layers to estimate the state of the smart grid for improved robustness against cyber-attacks. Other research contributions facilitate the management of cyber-security in the smart grid by presenting a distributed Software-Defined Network (SDN) architecture as shown in Figure 1 [14]. A distributed management framework was proposed in [15] to demonstrate its resilience over a centralized framework.

In recent work, we have built on our prior findings and introduced a proof of concept in to estimate the network state of the smart grid communication network, keeping the distributed software-defined network managed system [3]. The motivation for this study was the smart grid network state is vulnerable to uncertainties within the network and to adversaries that may modify communication network parameters to disrupt the operation of the smart grid network. In this paper, we move from proof of concept in [3] to develop (1) an implementation strategy for network state estimation, (2) an emulation environment for a given bus system, and (3) a performance analysis of the estimation and detection strategy. The key contributions of this paper are highlighted as follows:

- Emulated the network behavior in a False Data Injection (FDI) attack in the communication network layer of the smart grid;

- Developed a physics-based Network State Estimation (N-SE) model and a data-driven Ensemble CorrDet with Adaptive Network Statistics (ECD-ANS) model to detect FDI attacks in the communication network;
- Implemented a data fusion-based hybrid framework that combines both the physics-based NSE and the data-driven ECD-ANS models to enhance the detection of bad data.

The remaining sections of the paper are organized as follows. Section II presents the background of the network statistics of the communication network layer of the smart grid. The concept of the physics-based network state estimation (N-SE) model and the ECD-ANS approach are discussed. Section III provides a detailed description of the proposed hybrid framework for bad data detection. The numerical results from the case study are outlined in Section IV. The paper is finally concluded in Section V.

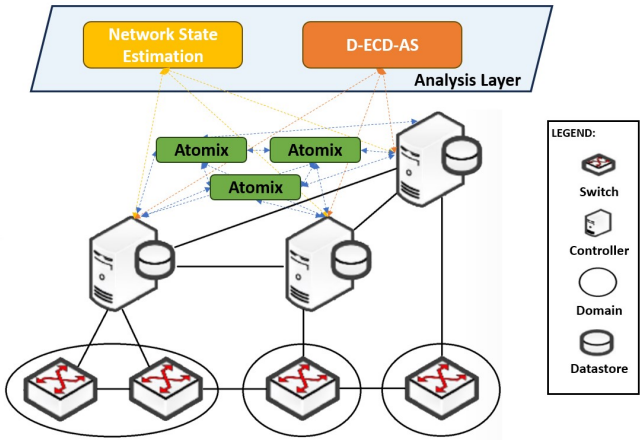

Fig. 1: Distributed, Flat SDN Controller Architecture used for Network State Estimation. (Proof of concept presented by the authors in [3])

II. Background Information

A. Performance Statistics in the Communication Network Layer

The communication network layer of the smart grid plays a crucial role in transmitting measurement data and control signals between various components of the grid. To ensure reliable operation and detect potential cyber-attacks, it is essential to monitor and analyze key performance statistics of the network. These statistics provide valuable insights into the network's state and can help identify anomalies or malicious activities. The following are some of the important network parameters considered in this study:

- Inter-arrival time (IAT): IAT represents the time elapsed between the arrival of two consecutive packets at a node. It provides information about the traffic patterns and load on the network. A shorter IAT indicates a higher traffic volume, while a longer IAT suggests lower traffic. Anomalies in IAT can indicate a potential FDI, Denial-of-Service (DoS) attack, or other network disruptions.
- Transmission delay (TD): TD is the time taken for a packet to be transmitted from the source to the destination node across the network. It is influenced by various factors such as network congestion, available bandwidth, distance between nodes, and processing delays. High transmission delays can indicate network congestion or potential routing issues, which may be caused by cyber-attacks.
- Packet count (PC): PC represents the total number of packets transmitted through the network over a specific period. It provides a measure of the traffic volume and can help detect sudden spikes or drops in network activity. Anomalies in packet count can indicate data injection or data theft attacks.
- Round-trip time (RTT): RTT is the time taken for a packet to travel from the source to the destination and back, including the time for the destination to process the packet and send an acknowledgment. It is a measure of the network's latency and responsiveness. High RTT values can indicate network congestion, long distances between nodes, or processing delays, potentially caused by cyber-attacks.
- Arrival rate (λ): The arrival rate represents the average number of packets arriving at a node per unit time. It is a key factor in determining the queuing delays and packet loss probabilities in the network. An abnormally high arrival rate can indicate a potential FDI or DoS attack, while a low arrival rate may suggest data suppression or tampering.
- Service rate (μ): The service rate represents the average number of packets that can be processed or transmitted by a node per unit time. It is determined by factors such as link bandwidth and processing capabilities of the nodes. The service rate affects the queuing delays and the overall throughput of the network. Anomalies in service rate can indicate resource exhaustion attacks or unauthorized changes to network configurations.

By continuously monitoring these performance statistics, the smart grid operators can gain valuable insights into the health and security of the communication network layer. Deviations from normal patterns or sudden changes in these parameters can alert the operators to potential cyber-attacks, enabling them to take timely corrective actions. The following sections discuss how physics-based state estimation models and data-driven machine learning approaches can leverage these network statistics to detect anomalies and enhance the cyber-physical security of the smart grid.

B. Physics-based State Estimation

Considering the communication network layer of the smart grid for state estimation, the classical Weighted Least Squares (WLS) approach is used due to its wide adoption in literature [11]. The communication network is modeled as a set of non-linear equations in Equation 1 based on the physics of the network [16].

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{1}$$

Where $\mathbf{z} = [z_1, z_2, ...z_m]^T \in \mathbb{R}^{1\times d}$ is the measurement vector from the communication network layer, $\mathbf{x} = [x_1, x_2, ...x_n]^T \in \mathbb{R}^{1\times N}$ is a vector of state variables, $h : \mathbb{R}^{1\times N} \rightarrow \mathbb{R}^{1\times d}$ is a non-linear differentiable function relating the measurements to the state variables and $\mathbf{e} = [e_1, e_2, ...e_m]^T \in \mathbb{R}^{1\times d}$ is the measurements error vector, where $\mathbf{e} \sim \mathcal{N}(0, \sigma^2)$. Each measurement error e_i is assumed to have a Gaussian distribution with zero mean and standard deviation, σ_i. Note that d is the number of measurements

comprising inter-arrival time, packet count, transmission delay, and round trip time. whereas N is the number of state variables consisting of arrival rate and service rate. These are all parameters from the communication network for state estimation.

The state variable vector from the communication network is defined as $\mathbf{x} = \begin{cases} \lambda \\ \mu \end{cases}$ which is obtained using the measurement vector $\mathbf{z} = \begin{cases} IAT \\ TD \\ PC \\ RTT \end{cases}$

The non-linear function that shows the relation between the state variable vector and the network measurements is provided in Equation 2 as in Equation 1.

$$\mathbf{z} = \begin{bmatrix} IAT \\ PC \\ TD \\ RTT \end{bmatrix} = \mathbf{h}(\mathbf{x}) + \mathbf{e} = \begin{bmatrix} \frac{1}{\lambda} \\ \lambda W \\ \frac{1}{\mu - \lambda} \\ \alpha + \frac{1}{\mu} + W_q \end{bmatrix} + \mathbf{e} \quad (2)$$

The mean waiting time in the communication network system is W and is expressed as $W = \frac{1}{\mu} + W_q$. The mean waiting time in the queue, Wq is expressed as $W_q = \frac{1}{\mu - \lambda}$ similar to [17]. The propagation delay is given as $\alpha = \frac{d}{s}$, where d is the distance traveled by a packet, and s is the wave propagation speed of the network link.

The communication network state estimation is formulated as a minimization problem in Equation 3 and solved with WLS to find the best estimate of the state variable vector.

$$J(\mathbf{x}) = [\mathbf{z} - h(\mathbf{x})]^T R^{-1} [\mathbf{z} - h(\mathbf{x})] \quad (3)$$

Where R^{-1} is the measurement weight matrix, and R is defined as the covariance matrix of the measurements. The standard deviation of each measurement, σ_i is assumed to be 0.5% of the measurement magnitude. The Newton-Raphson method is considered as the iterative approach to estimate the state variable by solving Equation 4 since the measurement model is non-linear.

$$\Delta\hat{\mathbf{x}} = (\mathbf{H}^T R^{-1} \mathbf{H})^{-1} \mathbf{H}^T R^{-1} \Delta\mathbf{z}. \quad (4)$$

Where $\mathbf{H} = \frac{\partial h}{\partial \mathbf{x}}$ is the Jacobian matrix of h at the current state estimation $\mathbf{x}^*$. $\Delta\mathbf{z} = \mathbf{z} - h(\mathbf{x}^*) = \mathbf{z} - \mathbf{z}^*$ and $\Delta\mathbf{x} = \mathbf{x} - \mathbf{x}^*$ are the correction of the measurement vector and state vector respectively. Equation 4 is solved in each iteration and a new estimate for the state variable is obtained in Equation 5 as follows.

$$\mathbf{x}^*_{new} = \mathbf{x}^* + \Delta\hat{\mathbf{x}}. \quad (5)$$

The iteration converges when $\Delta\hat{\mathbf{x}}$ in Equation 4 meets a minimum tolerance error value. After convergence, the final residual values in $r = \mathbf{z} - h(\hat{\mathbf{x}})$ are used for detecting malicious data. The bad data detection analysis is done with the statistical Chi-Squared test using Equation 6 since measurements are considered to be i.i.d.

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^{m} \left(\frac{z_i - h_i \hat{\mathbf{x}}}{\sigma_i} \right)^2 \underset{<}{>} \chi^2_{(d-N),p} \quad (6)$$

Where m is the number of samples, $(d - N)$ denotes the degrees of freedom and p is the probability with a value of 0.95. An incoming sample is predicted to be anomalous if $J(\hat{\mathbf{x}})$ is greater than the Chi-squared threshold, $\chi^2_{(d-N),p}$, and vice versa.

C. Ensemble CorrDet with Adaptive Statistics

The machine learning model considered for this work is the Ensemble CorrDet with Adaptive Statistics. ECD-AS is used to learn from the network measurements to detect abnormal behavior in the communication network. ECD-AS is an extension of the CorrDet algorithm described in [18], which assumes local CorrDet detectors with each corresponding to a node for a local region to detect anomalies, then updates the cloud layer to identify and isolate errors. ECD-AS first learns the network statistics of the normal samples by obtaining the mean, μ_m and inverse covariance matrix, $\mathbf{\Sigma}_m^{-1}$ for training. The estimated parameters are then used in the testing phase. These are used as initialization for the testing phase. As new samples, m arrive, the statistics are adapted to accommodate the dynamics in the network measurements. The squared Mahalanobis distance, $\delta^{ECD}(\mathbf{z})$ for the sample is obtained using Equation 7.

$$\delta^{ECD}(\mathbf{z}) = (\mathbf{z}_m - \mu_m)^T \Sigma_m^{-1} (\mathbf{z}_m - \mu_m) \quad (7)$$

Similar to the SE model, we conduct a Chi-Squared test to detect abnormal behavior of the communication network. The squared Mahalanobis distance, $\delta^{ECD}(\mathbf{z})$ is compared with the Chi-Squared threshold, $\chi^2_{(d-N),p}$.

$$\delta^{ECD}(\mathbf{z}) = (\mathbf{z}_m - \mu_m)^T \Sigma_m^{-1} (\mathbf{z}_m - \mu_m) \underset{<}{>} \chi^2_{(d-N),p} \quad (8)$$

$$z = \begin{cases} Anomalous, & \text{if } \delta^{\mathbf{ECD}}(\mathbf{z}) > \chi^2_{(2(d-N)),p} \\ Normal, & \text{if } \delta^{\mathbf{ECD}}(\mathbf{z}) < \chi^2_{(2(d-N)),p} \end{cases} \quad (9)$$

If the decision score, $\delta^{ECD}(\mathbf{z})$ is greater than the Chi-Squared threshold, $\chi^2_{(d-N),p}$, then the sample is flagged to be anomalous. Otherwise, it is considered normal if it is below the threshold value. To reflect the dynamics in the network measurements, the statistics which are mean, μ_m and inverse covariance matrix, $\mathbf{\Sigma}_m^{-1}$ are updated using Equations 10 and 11. Where α is a hyper-parameter between 0 and 1 obtained from experimentation and determines the significance of a new sample.

$$\mu_{m,new} = (1 - \alpha)\mu_m + \alpha(z_m - \mu_m \quad (10)$$

$$\Sigma^{-1}_{m,new} = \frac{1}{1 - \alpha} \left(\Sigma_m^{-1} - \frac{(z_m - \mu_m)(z_m - \mu_m)^T}{\frac{1-\alpha}{\alpha} + (z_m - \mu_m)(z_m - \mu_m)^T} \right) \quad (11)$$

III. Bad Data Detection: Hybrid Physics-based Data-Driven Model

This work introduces a novel approach by changing the state estimation focus to the smart grid network state and by integrating the physics-based network state estimation (N-SE) model with an updated data-driven Ensemble CorrDet with Adaptive Network Statistics (ECD-ANS) model defined in Sections II-B and II-C. The purpose of combining the two models is to leverage their capabilities to enhance anomaly detection in the communication network layer of the smart grid. The decision scores $J(\hat{\mathbf{x}})$ and $\delta^{ECD}(\mathbf{z})$ from the physics-based N-SE and data-driven ECD-ANS models respectively are fused to form a combined distance measure. The decision score of the physics-based N-SE model is defined in Equation 12 as follows.

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^{m} \left(\frac{z_i - h_i(\hat{\mathbf{x}})}{\sigma_i} \right)^2 \tag{12}$$

The N-SE portion of the combined distance measure is obtained individually per sample as described in Section II-B. A bad data is detected if the decision score, $J(\hat{\mathbf{x}})$ exceeds the Chi-Squared threshold, $\chi^2_{(d-N),p}$.

The decision score of the data-driven ECD-ANS model is provided in the following equation.

$$\delta^{ECD}(\mathbf{z}) = \sum_{i=1}^{m} \left(\frac{z_i - \mu_i}{\sigma_i} \right)^2 \tag{13}$$

The squared Mahalanobis distance, $\delta^{ECD}(\mathbf{z})$ discussed in II-C forms the remaining part of the combined distance measure. An incoming sample is detected to be anomalous if the decision variable is above the Chi-Squared threshold, $\chi^2_{(d-N),p}$.

For a new incoming sample, data fusion of the decision scores is done by summing up $J(\hat{\mathbf{x}})$ and $\delta^{ECD}(\mathbf{z})$ of the two models. The combined decision score is given in Equation 14.

$$\mathbf{J}_{comb} = J(\hat{\mathbf{x}}) + \delta^{ECD}(\mathbf{z}) \tag{14}$$

The proposed hybrid physics-based data-driven model uses an augmented Chi-Squared test for anomaly detection in the communication network layer of the smart grid. The combined decision score, $\mathbf{J}_{comb}$ is compared with a Chi-Squared threshold, $\chi^2_{(2(d-N)),p}$.

$$\mathbf{J}_{comb} = J(\hat{\mathbf{x}}) + \delta^{ECD}(\mathbf{z}) > \chi^2_{(2(d-N)),p} \tag{15}$$

$$z = \begin{cases} Anomalous, & \text{if } \mathbf{J}_{comb} > \chi^2_{(2(d-N)),p} \\ Normal, & \text{if } \mathbf{J}_{comb} < \chi^2_{(2(d-N)),p} \end{cases} \tag{16}$$

A sample is flagged as anomalous if the combined decision variable, $\mathbf{J}_{comb}$ is larger than the Chi-Squared threshold, $\chi^2_{(2(d-N)),p}$. If the decision variable is below the defined threshold, the sample is considered normal.

IV. Case Study Implementation

In this work, the models presented for detecting anomalous data in the communication network of the smart grid are evaluated using the 14-bus network architecture comprising 14 nodes shown in Figure 2. The discrete-event simulation framework, SimComponent, and SimPy libraries are utilized to replicate the network traffic of the communication network layer of the smart grid. The measurement samples of the communication network are generated using the algorithm described in our previous work [3]. Using the SimPy environment, the packet generator is used to generate packets with exponential inter-arrival times and exponentially distributed packet sizes with defined port rates and queue limits following the $M/M/c$ queuing model where c$\geq$1 as in [19]. The packet sink records the network measurements consisting of inter-arrival time, transmission delay, packet count, and round-trip time. The dataset consists of 46 samples and each sample has 164 measurements giving a total of $7,544$ measurements. A Gaussian noise with zero mean and 0.005 standard deviation is added to the measurements set to introduce uncertainties.

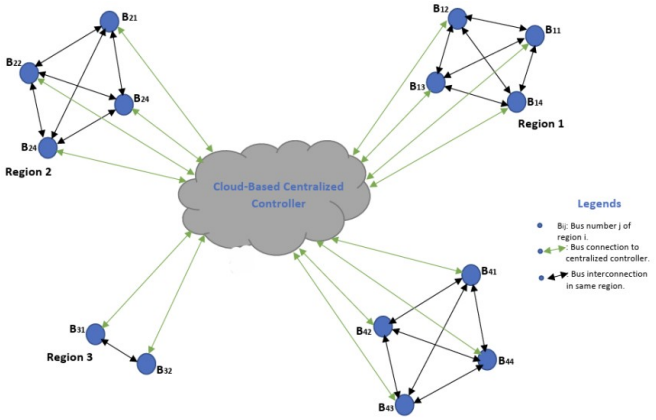

Fig. 2: 14 Bus Network Architecture [3]

False Data Injection (FDI) attack in the smart grid targeting the N-SE involves altering the measurements being sent to the N-SE to mislead it in control decisions. FDI attacks affect the behavior of the network parameters including our selected measurement variables and its effect can cause an increase in these parameters such as high transmission delays. This poses significant threats, especially for such time-critical systems. The FDI attack is implemented in this work by injecting an error which is a Gaussian noise with zero mean and standard deviation of 5% of the measurement magnitude. The error is added to a randomly selected measurement for 10 consecutive samples ranging from $11-20$. The size of the measurement vector per sample, d is 164 and that of the state variable vector, N is 82, which gives the degree of freedom $(d-N)$ as 82. Considering a confidence level of 95% gives the Chi-Squared threshold value, $\chi^2_{(d-N),p}$ for the physics-based and the data-driven ECD-AS models to be 114.6949. For the augmented Chi-Squared test, the measurement vector size per sample, d is 328 and that of the state variable vector size, N is 164, which gives the degree of freedom $(d-N)$ as 164. A confidence level of 95% gives the Chi-Squared threshold value, $\chi^2_{(2(d-N)),p}$ for the hybrid physics-based data-driven ECD-ANS model to be 209.0474.

The results for the models in detecting FDI attacks are shown in Figure 3. The graph plots in Figures 3(a.i)-(a.iii) illustrate the prediction outcome of FDI attack detection on the samples for the physics-based N-SE, data-driven ECD-ANS, and hybrid physics-based data-driven model respectively. The red line in the plots denotes the Chi-Squared threshold. Samples exceeding the threshold value show anomalous sample predictions, while samples below the threshold value imply normal sample predictions. A confusion matrix is used to describe the models' performances in classifying the datasets, as seen in Figures 3(b.i)-(b.iii) for the physics-based N-SE, data-driven ECD-ANS, and hybrid physics-based data-driven model respectively. It shows the four outcomes for each model. True Positives (TP) are instances where normal samples are predicted to be normal. True Negatives (TN) are instances where anomalous samples are predicted to be anomalous. False Positives (FP) are instances where anomalous samples are predicted to be normal while False Negatives (FN) are instances where normal samples are predicted to be anomalous. The physics-based N-SE has 36 TPs, 2 TNs, 0 FN and 8 FPs. The data-driven ECD-ANS has 36 TPs, 3 TNs, 0 FN and 7 FPs. The hybrid physics-based data-driven model has 36 TPs, 8 TNs, 0 FN, and 2 FPs. Based on these, it is evident from Figure 3 that the proposed hybrid physics-based data-driven ECD-AS model outperforms the standalone methods by demonstrating high values for TP and TN with extremely low values for FP and FN. The data-driven ECD-AS model has slightly higher performance than the physics-based model in terms of TN and FP. The metrics considered for evaluating the performance of the models are accuracy, precision, recall, and f1-score, and these are presented in Table I. Accuracy is the ratio of correct predictions to the total number of predictions as seen in Equation 17.

$$\frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

Accuracy is a very good metric in the case where datasets have balanced class sizes. However, in the real world, the number of anomalous measurements is smaller than the normal measurements. This implies that the measurements are typically imbalanced in nature. Similarly, the datasets used in this work are imbalanced. Hence accuracy as a metric can be misleading and is not good at predicting the minority class. For a comprehensive view of the performance of the models in detecting bad data, we include additional metrics which are precision, recall, and f1-score. Precision is the ratio of correctly predicted normal samples to the total predicted normal samples. It gives the proportion of predicted normal samples that are correct out of all the predicted normal samples. Precision is used when minimizing FP is important.

$$\frac{TP}{TP + FP} \tag{18}$$

Recall is the ratio of the correctly predicted normal samples to the actual normal samples. This shows how the model performs in correctly predicting normal samples. Recall is used when minimizing FN is critical. The expression for recall is given as follows.

$$\frac{TP}{TP + FN} \tag{19}$$

F1-score is the harmonic mean of precision and recall, as provided in Equation 19. It assesses the general performance of the model. F1-score balances precision and recall, and it is useful to achieve a tradeoff between minimizing FP and FN.

$$\frac{2 * Precision * Recall}{Precision + Recall} \tag{20}$$

The data-driven ECD-AS model shows a moderate increase in f1-score than the physics-based SE model. In all instances in the classification report, the proposed hybrid physics-based data-driven ECD-ANS model demonstrates the highest performance in detecting normal or anomalous data than the state-of-the-art SE and ECD-AS methods. The f1-score of the proposed model in detecting anomalous data is twice the standalone methods while yielding the highest performance to indicate its ability to classify TP and TN. In general, the proposed hybrid physics-based data-driven ECD-ANS model enhances the detection of FDI attacks than the standalone physics-based N-SE and ECD-ANS models.

V. Conclusion

This paper focuses on estimating the state of the communication network layer of the smart grid, which is a novel concept. To extend our previous work which demonstrated the proof of concept, we have implemented a hybrid physics-based data-driven ECD-ANS model that utilizes the spatial and temporal characteristics of both the physics-based N-SE and the ECD-ANS models. A case study is presented to analyze the performance of the proposed model in detecting FDI attacks. We implemented an FDI attack by modifying the measurements used in state estimation. An augmented Chi-Squared test is conducted to detect errors in the network measurements. The proposed method combines the decision scores from the physics-based SE and the data-driven ECD-AS model for bad data detection. The simulation results show that the proposed model has the best overall performance in detecting the FDI attack. This proves that the proposed model can improve the detection of cyber threats like FDI to boost the cyber-physical security of the communication network layer of the smart grid.

References

[1] M. Abdel-Nasser, K. Mahmoud, and H. Kashef, "A novel smart grid state estimation method based on neural networks," *IJIMAI*, vol. 5, no. 1, pp. 92–100, 2018.

[2] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 476–486, 2011.

[3] R. Mathieu, S. Boamah, A. Cooper, D. Agnew, J. McNair, and A. Bretas, "Communication network layer state estimation measurement model for a cyber-secure smart grid," in *2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2024, pp. 1–5.

[4] R. D. Trevizan, C. Ruben, K. Nagaraj, L. L. Ibukun, A. C. Starke, A. S. Bretas, J. McNair, and A. Zare, "Data-driven physics-based solution for false data injection diagnosis in smart grids," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[5] T. Zou, N. Aljohani, K. Nagaraj, S. Zou, C. Ruben, A. Bretas, A. Zare, and J. McNair, "A network parameter database false data injection correction physics-based model: A machine learning synthetic measurement-based approach," *Applied Sciences*, vol. 11, no. 17, p. 8074, 2021.

[6] T. Liu and T. Shu, "On the security of ann-based ac state estimation in smart grid," *Computers & Security*, vol. 105, p. 102265, 2021.

[7] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture gaussian distribution learning method," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161–171, 2017.

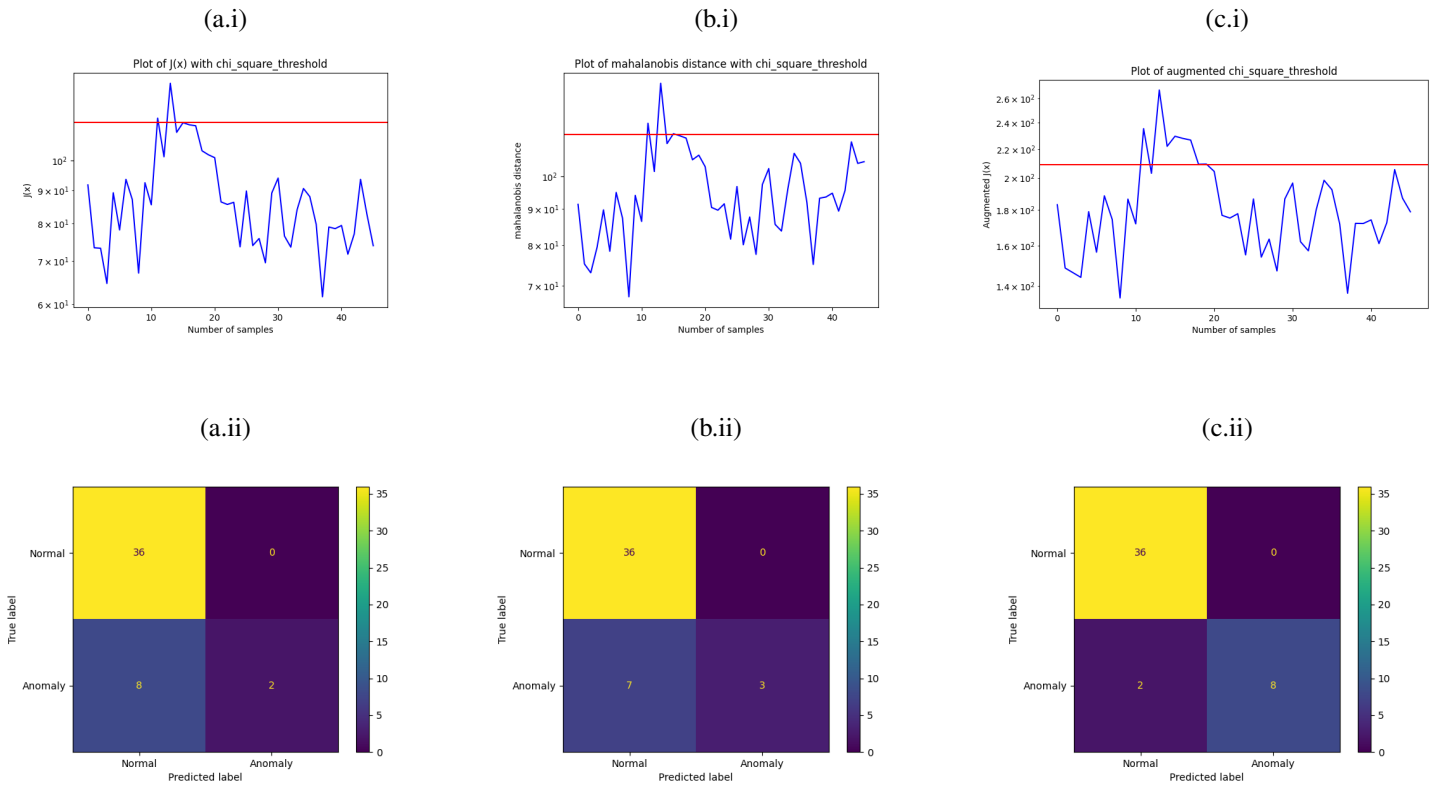

Fig. 3: Comparison of Physics-based N-SE, Data-driven ECD-ANS and Hybrid Physics-based Data-driven models for detecting FDI attacks

Models	Class	Accuracy	Precision	Recall	F1-Score
Physics-based N-SE	Normal Anomalous	83	82 100	100 20	90 33
Data-driven ECD-ANS	Normal Anomalous	85	84 100	100 30	91 46
Hybrid physics-based data-driven ECD-ANS	Normal Anomalous	96	95 100	100 80	97 89

TABLE I: Performance of models in detecting FDI dttack

[8] K. Nagaraj, N. Aljohani, S. Zou, C. Ruben, A. Bretas, A. Zare, and J. McNair, "State estimator and machine learning analysis of residual differences to detect and identify fdi and parameter errors in smart grids," in *2020 52nd North American Power Symposium (NAPS)*. IEEE, 2021, pp. 1–6.

[9] F. Ahmad, A. Rasool, E. Ozsoy, R. Sekar, A. Sabanovic, and M. Elitaş, "Distribution system state estimation-a step towards smart grid," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 2659–2671, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032117310134

[10] V. Vega-Martinez, A. Cooper, B. Vera, N. Aljohani, and A. Bretas, "Hybrid data-driven physics-based model framework implementation: Towards a secure cyber-physical operation of the smart grid," in *2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*. IEEE, 2022, pp. 1–5.

[11] M. M. Rana, W. Xiang, and E. Wang, "Smart grid state estimation and stabilisation," *International journal of electrical power & energy systems*, vol. 102, pp. 152–159, 2018.

[12] N. Aljohani, D. Agnew, K. Nagaraj, S. A. Boamah, R. Mathieu, A. S. Bretas, J. McNair, and A. Zare, "Cross-layered cyber-physical power system state estimation towards a secure grid operation," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2022, pp. 1–5.

[13] 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.

[14] D. Agnew, N. Aljohani, R. Mathieu, S. Boamah, K. Nagaraj, J. McNair, and A. Bretas, "Implementation aspects of smart grids cyber-security cross-layered framework for critical infrastructure operation," *Applied Sciences*, vol. 12, no. 14, p. 6868, 2022.

[15] D. Agnew, S. Boamah, R. Mathieu, A. Cooper, J. McNair, and A. Bretas, "Distributed software-defined network architecture for smart grid resilience to denial-of-service attacks," in *2023 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2023, pp. 1–5.

[16] A. Bretas, N. Bretas, J. B. London Jr, and B. Carvalho, *Cyber-physical power systems state estimation*. Elsevier, 2021.

[17] J. F. Shortle, J. M. Thompson, D. Gross, and C. M. Harris, *Fundamentals of queueing theory*. John Wiley & Sons, 2018, vol. 399.

[18] 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.

[19] 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. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/stg2.12070