Power Data Quality Improvement Through PMU Bad Data Detection Based on Deep Complex Network

[1]PREETI KABRA, [2]D SUDHA RANI
[1]K L University, Vijaywada, Andhra Pradesh, INDIA
[2]Sri vasavi college of Engineering, Tadepalligundem, Andhra Pradesh, INDIA

Abstract- Phasor Measurement Units (PMUs) enable the switching of devices in various power signal modes. A jitter or glitch in a signal cause bad data and also the PMU data will spike due to a disturbance or a transmitting data mistake. As a result of these difficulties, PMU data suffer from different degrees of data quality problems. To detect the bad data, several approaches have been already utilized however it provides some disadvantages such as complexity due to the utilization of dual identical systems separately for analyzing both real and imaginary values of PMU. Likewise, the bad data due to the topology variations have not been optimally identified. To overcome these issues a Robust Bad Data Detection Technique has been proposed in which a Deep complex neural network (DCNN) is incorporated to process the complex number having both voltage magnitude and phase angle. Deep complex Networks are also proposed with the conjunction of topology processor and AC state estimator (SE). Moreover, instead of Batch normalization weight normalization is altered due to the fusion of recurrent timestamps for measuring voltage magnitude and phase angle. The comparative analysis is done in terms of accuracy , Bad data detection capability , bad data detection range and running time with existing techniques The proposed technique provides accuracy of about 99.5% which is higher than the existing techniques.

Keywords- Phasor Measurement Units (PMUs), Bad Data, Deep Complex Neural Network (DCNN), State Estimator(SE), Weight Normalization, Batch Normalization.

Received: August 28, 2021. Revised: April 21, 2022. Accepted: May 21, 2022. Published: June 25, 2022.

Nomenclature
$\boldsymbol{P_{nn}}$ *bus admittance matrix of the AC power system*
Ii and Vi *net current and voltage at the ith bus*
$\boldsymbol{V^U V^{NU}}$ *voltage vectors for PMU and non-PMU buses,*
$\boldsymbol{P^U}$ $\boldsymbol{P^{NU}}$ *bus admittance sub-matrices for various PMU and non-PMU buses*
$\boldsymbol{I_n}$ *net current vector.*
$\boldsymbol{x}$,$\boldsymbol{y}$ *real vectors*
$\boldsymbol{w_{ij}}$ *weights associated with the bad data detection*
$\boldsymbol{b_i}$, $\boldsymbol{\vartheta_I}$ *affine relationship between the mean-variance.*
$\boldsymbol{I}$ *Imaginary Value*
$\boldsymbol{R}$ *Real value*
$\boldsymbol{o_j}$ *output of convolutional layer*
$\boldsymbol{\gamma_j \beta_j}$ *optional parameters for convolutional layer*
$\in$ *used for numerical stability*
$\boldsymbol{W}$ *represents the layer weights*
$\boldsymbol{W_J}$ *represents the norm of weights for the output channel*
$*$ *denotes the convolution*

1. Introduction

Power system security is greatly improved by accurately analyzing the current operating status in real-time. A power grid is a network of interconnected power lines that transmit energy from generators to users. Power networks may cover whole nations or regions and come in a range of sizes. Because of the growing need for energy, power distribution networks must be transformed into networks that combine diverse kinds of energy generation as well as distribution. Loads and generators connected to the grid both have an impact on power performance. Due to their speed, synchronism, and precision, phasor measurement units (PMUs) have become a fundamental mechanism utilized in pervasive electronics to accomplish state perception [1]. A phasor measuring unit (PMU) is a tool utilized within a power grid that determines both the magnitude and phase angle of such an electrical phasor element (like voltage or current) utilizing a shared time source for timing. PMUs may also supply real-time phasor time data for important power system applications including corrective action schemes, oscillation detection, and condition estimates [2-6].

Numerous academics have examined the false data issue in PMU assessments out from the viewpoints of cyber assault and signal processing flaws, and have proposed several solutions. However, it is also stated that in spite of repeated information assaults, both computation cost or temporal difficulty of a filter would rise, rendering it inappropriate for real-time use. PMU data is sensitive to a variety of variables due to the complexity of the components [7]. A jitter in a global positioning system (GPS) signal, for example, might produce phase angle variation. It's also conceivable that PMU data will surge as a result of interference or a data transmission error. PMU data suffer from varying degrees of data quality concerns as a result of these issues. According to the California Independent System Operator's (ISO) Five-Year Plan, around 10% to 17% of PMU data in US has issues [8]. PMUs are utilized in Energy Management Systems to improve the state estimation functionality (EMS). The simulation model starts by collecting completely viewable assessment data from the system, i.e. necessary qualities of voltages and currents in the system are detected and given to the State Estimator to compute the fundamental values of the overall network. PMU measurements are commonly distorted as a result of (a) deliberate data corruption by a cyber-assault or (b) inadvertent data corruption over the digital data processing, storage, and retrieval stage [9–11]. Data quality concerns make the system less visible, impair the effectiveness of state estimates and parameter identification using PMUs, and potentially jeopardize power system safety and stability. PMU poor data detection has become a significant issue, and it is vital for increasing data quality and guaranteeing correct state perception.

Several approaches for detecting bad data in power systems have been presented. The singularity of the impedance matrix and the sparsity of the error vector are exploited in [12] to propose a new technique for detecting measurement errors in DC power flow. It makes use of the power system's structure to correctly compute measurement errors. A poor data detection technique based on state estimate is given in [13]. By identifying angle biases and current scaling errors, the phasor-measurement-based state estimator enhances data consistency. [14] introduces a time-series prediction model with a Kalman filter and smoothing method for cleaning poor data. [15] provides a technique for detecting incorrect data in real-time that uses an unscented Kalman filter in combination with a state estimation algorithm. Various academics had concentrated on developing reduced and highly secure connections for such purposes. Nevertheless, because of constraints in legacy technology used in many power stations, bad data detection is typically only offered at the central level. A linear weighted least square-based state estimation method may detect incorrect data from defective current transformers, according to [16].

To identify fake data in PMU measurements, most false data detection algorithms need SCADA measurements. Furthermore, current research indicates that PMU measurements are not completely safe against cyber assaults [17–19]. An attacker manipulates the measurements of the PMU as well as the adjacent SCADA meters (RTUs) in the case of an FDIA on the PMU measurements such that corrupt values pass the measurement residual-based checks [20] at the energy control centre and the attack is disguised [21-22]. As a result, standard techniques for detecting, identifying, and correcting incorrect data are ineffective in detecting purposeful misleading data in PMU measurements.

In the case of accidental data corruption, the inherent high noise level in SCADA measurements, low sample rate, and lack of time-stamping render SCADA measurements unsuitable for faulty data detection in sparsely located PMU measurements. Apart from cyber assaults, accidental FDI can occur owing to defective current or potential transformers, noise in the communication channel, GPS jamming, and other factors [23-25]. As a result, an alternate method for detecting both deliberate and inadvertent misleading data in PMU measurements has to be developed.

The Contribution of this paper includes,

- a deep complex neural network to handle complex values include both voltage magnitude as well as phase angle as a whole.
- Rather than using batch normalization, weight normalization has already been added as a result of the merging between repeated timestamps for monitoring voltage magnitude and phase angle, which may significantly enhance the model's training performance.
- A deep complex network has been utilized with the conjunction of a topology processor and AC state estimator, topology processors detect substantial information about the network topology to recognize faulty data caused by topology change caused by disruptions.

The content of the paper is organized as follows: section 1 represents the introduction; section 2 presents the related work; the novel solutions are presented in section 3; the implementation results and its comparison are provided in section 4; finally, section 5 concludes the paper.

2. Literature Survey

Amutha, et al [26] aimed at detecting abnormalities in streaming PMU multivariate information in smart grid by taking into account all attributes utilizing the Density Estimation Technique depending on Gaussian Mixture Theory. The suggested architecture has been evaluated in both offline as well as online forms of data streams, but also the research findings show that the suggested technique performs competently in identification. This methodology has a lower false positive as well as false-negative rate, it may be used for real-time anomaly monitoring. The suggested model is additionally validated for streaming data scenarios by being evaluated to current research in respect of the accuracy, recall, and F1 score.

Zhou, et al [27] Utilizing online learning and a multivariate data-drift detection technique, a unique device-level deep learning-based data-driven strategy for anomaly detection, localization, and classification over streaming PMU data is proposed. Dynamic data Change Driven Learning (DCDL) but also Continuity Driven Learning (CDL) are presented as well as contrasted as PMUNET variations. The DCDL technique surpasses the CDL as well as similar standard approaches. Thus the suggested methodology in this paper efficiently detects the data anomalies.

Rehan, et al [28] An efficient attack strategy has been proposed to detect the false data injected into the power system. Using linear regression the false data is injected into the power system,also it is used by FDI to create any assault which could overcome BDD but also SVM-based defence technologies. Monitoring intelligent grid assaults allows us to ensure that command choices in the control room are predicated upon trustworthy assessments and that deceptive information is eliminated resulting in computing complexity.

Yang, et al [29] A data-driven PMU poor data identification technique based on spectral clustering utilizing single PMU data is presented to improve PMU data quality. The topology and characteristics of the system are not required by the suggested approach. First, utilizing the slope characteristic of each data, a data identification technique based on a decision tree is presented to identify event data from bad data. Then, using spectral clustering, a technique for detecting faulty data is devised. This approach can detect faulty data with a minor variation by evaluating the weighted relationships among all the data.

Jovicic, et al [30] A linear approach is provided for state estimate of power systems that are monitored using both conventional and synchrophasor measurements, including bad data detection. Both forms of data are processed at the same time, with states approximated in rectangular coordinates. The linear weighted least square approach is used to create the suggested estimator. The network is represented in terms of voltages and currents in the rectangular form to permit the generation of linear measurement functions, and pseudo-measurements are employed to simulate traditional measurements. Furthermore, to detect faulty data, the biggest normalized residual test is utilized.

In [26] difficulty in handling bad data .[27] detects data anomalies.[28] analyzes about the computing complexity . The paper [29] detect the faulty data with some minor variation only. To detect faulty data , the bigget normalized residual test is used which is complex [30]. To overcome the above mentioned issues a robust methodology is proposed which is explained in the upcoming section.

3. Bad Data Detection Using Deep Complex Network

PMUs are used to measure the phasor quantity in the grid system. Because of the glitch or ripple, it produces false or bad data at the output.These anomaly may reduce the accuracy of the of the system and leads to performance degradation . Dual identical models were used for analyzing the real and imaginary data PMU independently which increases the difficulty in computational process also the phase angle variations may cause false data occurrence. Similarly, poor data owing to topology changes have not been adequately detected using simply the AC state estimator. As a result, a Robust Bad Data Technique was designed which uses a deep complex neural network to process complex numbers with both voltage magnitude and phase angle overall. Weight normalization has been integrated into the deep complex neural network owing to the fusion of recurrent timestamps for monitoring voltage, magnitude and phase angle, which may further enhance model training efficiency. With the help of prior data measured of smaller complexity, the proposed deep complex neural network recognizes false information in PMU assessments.As a result, the suggested deep complex network has been used in conjunction with a topology processor and an AC state estimator, with the topology processor recognizing substantial changes in the network topology to achieve incorrect data identification owing to topology variation caused by disturbances. Bad data in the multiple PMU power grid networks may be rectified correctly using the proposed methodology. The Data neural Network consists of the hidden layer which may perform the exactly needed function of the proposed so that the required output can be obtained without any fault. The Robust bad data detection technique with its concept which is incorporated in it has been clearly shown below in figure 1.

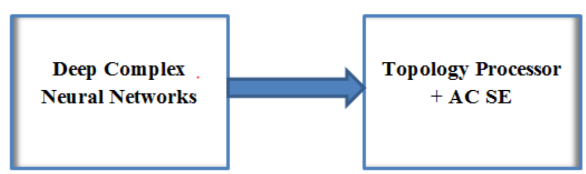
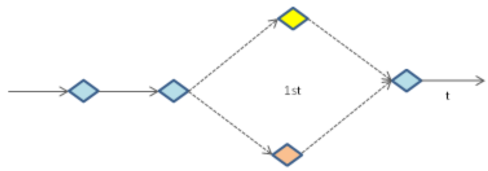


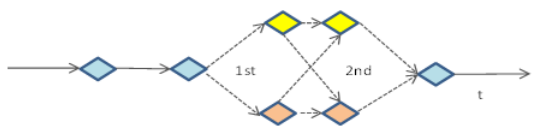
Figure 1: Robust bad data detection Technique overview

3.1 Bad Data Occurrence

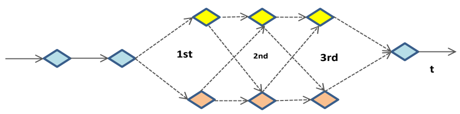
The Bad data deviates from the normal data. After evaluating a substantial portion of data obtained, it was discovered that the majority of the bad data occurs on its own and that the amount of adjacent bad data seems to be no over than three. It is also mentioned that the exceptions are all separated not even in order. As an example, consider the magnitude. This may be used for calculating amplitude, frequency, and rate of change in frequency, where magnitude includes voltage as well as current magnitude. The schematic representation of Multiple Bad data occurrences is shown in figure 2



(a)



(b)



(c)

Figure 2: A diagram of (a) 1 Bad data (b) 2 Bad data and (c) 3 Bad data

The bad data occurs in the input data itself due to the occurrence of many inteferences such as glitch etc.The bad data may includes normal data, irregularity data with higher magnitude and irregularity data with lower magnitude.These bad datas are differentiated by different colours.The blue colour signifies normal data. The yellow colour signifies the irregularity data with a higher magnitude and the orange colour represents the irregularity data with a lower amplitude. The number of contiguous bad data maybe 1 or 2 or 3 as represented in figure 2. This is how the bad data initially occur in the source system.

3.2 Model of an AC System

For n bus, AC power structure, the nodal expression processed utilizing Ohm's Law is as follows

$$\begin{bmatrix} \boldsymbol{I_1} \\ \boldsymbol{I_2} \\ \boldsymbol{I_3} \\ \vdots \\ \boldsymbol{I_n} \end{bmatrix} = \begin{bmatrix} \boldsymbol{P_{11}} & \boldsymbol{P_{12}} & \dots & \boldsymbol{P_{1n}} \\ \boldsymbol{P_{21}} & \boldsymbol{P_{22}} & \dots & \boldsymbol{P_{2n}} \\ \boldsymbol{P_{31}} & \boldsymbol{P_{32}} & \dots & \boldsymbol{P_{3n}} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{P_{n1}} & \boldsymbol{P_{n2}} & \dots & \boldsymbol{P_{nn}} \end{bmatrix} \begin{bmatrix} \boldsymbol{V_1} \\ \boldsymbol{V_2} \\ \boldsymbol{V_3} \\ \vdots \\ \boldsymbol{V_n} \end{bmatrix} \dots\dots\dots (1)$$

where Ii and Vi were the net current and voltage at the ith bus, respectively. Pn×n denotes the bus admittance matrix of the AC power system having (i,j) th element being Pij. If there are m PMUs mounted in the system. Here equation 1 can be written as

$$[\boldsymbol{I}] = [\boldsymbol{P^U} \quad \boldsymbol{P^{NU}}] \begin{bmatrix} V^U \\ V^{NU} \end{bmatrix} \dots\dots\dots\dots\dots (2)$$

Here $\boldsymbol{V^U}$m×1 and $\boldsymbol{V^{NU}}$ (n m)×1 represents the voltage vectors for PMU and non-PMU buses, correspondingly. The admittances between the various PMU as well as non-PMU buses were characterized by the associated bus admittance sub-matrices PU n×m and $\boldsymbol{P^{NU}}$n×(nm). I n×1 is the net current vector. Then formula 2 can be rewritten as

$$P^U V^U + P^{NU} V^{NU} - I = 0 \dots\dots\dots\dots\dots\dots (3)$$

If $(P^{NU} V^{NU} - I)$ can be substituted by M and also σ which is the mean and variance vector correspondingly.

$$P^U V^U + M \pm \sigma = 0 \dots\dots\dots\dots\dots\dots\dots (4)$$

Although equation 4 depicts a non-linear network, this simply offers a linear input connection between the voltages of the PMU buses. Those must be stressed since the basic link between M and σ in equation 4 is unknown. The deterministic optimization method for determining M and σ in equation 2 is to utilize the historical real-time/dynamic SE results from the corresponding mean and variance vectors of $P^{NU} V^{NU}$and I.

3.3 Function of Deep Neural Networks with State Estimator

A PMU provides the phasor quantity such as the voltage magnitude and the associated phase angle of the voltage To deal with the complex voltages the deep complex neural networks along with the AC system model has been incorporated. Each deep complex neural network model is trained in a way so that it can linearly express the ith PMU bus voltage measurement in terms of other (m - 1) PMU bus voltage measurements.

The relationship with the AC system model with the bad data detection is given using the expression,

$$V_{i=-} \left[\sum_{\substack{j=1 \\ j \neq i}}^{m} P_{ij} V_j + M_i \pm \sigma_I \right] Y_{ii}^{-1} \dots\dots\dots\dots (5)$$

Hence the above-mentioned equation has been replaced by the weight terms and the affine relationship between the variance were given as,

$$\sum_{\substack{j=1 \\ j \neq i}}^{m} w_{ij} V_j + b_i \pm \vartheta_I \quad \forall_i = 1 \dots \dots \dots m \dots (6)$$

Where w_{ij} are the weights associated with the bad data detection b_i and ϑ_I were the affine relationship between the mean-variance.

Normally, the system gets complicated due to the utilization of 2m number of systems from the number of PMUs. Hence in this proposed model we are utilizing m models from PMUs in deep neural network through the mathematical concept called the convolution of complex numbers for both Real as well as imaginary numbers. Hence the complexity has been reduced.

Every Complex number has both the real part as well as the imaginary part. Here the convolution of the complex filter matrix along with the complex vector is performed where

C=A+iB………………………….. (7)

And the complex vector is given as h= x+iy. In this A and B are the Real matrices and x and y are the real vectors. The convolution operator is always distributive

$$C * h = (A * x - B * y) + i (B * x + A * y) \dots\dots\dots (8)$$

Rewriting the convolution terms employing Matrix as follows,

$$\begin{bmatrix} R & (C * h) \\ I & (C * h) \end{bmatrix} = \begin{bmatrix} A & -B \\ B & A \end{bmatrix} * \begin{bmatrix} x \\ y \end{bmatrix} \dots\dots (9)$$

Here R means the Real value represents the Value of the

Voltage Magnitude and then the I, the Imaginary Value represents the Phase angle value in the above-mentioned equation.

By using this convolution form in the deep neural networks, providing the Voltage magnitude and the phase angle in the single system provides the output efficiently. Hence the complexity gets reduced due to the availability of a single system in the proposed methodology. The Bad data Occurrence may happen at any time so the detection of Bad data process is time-dependent. It has to be detected in a periodical manner. The Batch Normalization approach towards speeding neural network training by normalizing its signal density for every level. But in this proposed system we are concern about the periodicity in the detection of bad data that is not achieved by the BN so we are utilizing the Weight normalization method. The WN is an alternative for BN. It utilizes implicit normalization, that leads inside the standard of both the outcome having nearly identical to the current standard of the source. Weights, for instance, should be normalized and multiplied by a learnt scaling parameter for the convolutional layer:

$$o_j = \gamma_j \frac{W_j * x}{\|W_J\|_F + \epsilon} + \beta_j \qquad \ldots\ldots\ldots\ldots\ldots\ldots (10)$$

where o_j represents the output, $\gamma_j \beta_j$ were the optional parameters, ∈ used for numerical stability, W represents the layer weights, W_J represents the norm of weights for the output channel and $*$ denotes the convolution. The flow chart explains the entire proposed system as follows,

Weight normalization has been used in the proposed methodology due to the fusion of recurrent timestamps for measuring voltage magnitude and phase angle. We have overcome the disadvantage by using weight normalization. The Flow chart for the entire Bad data processing for the novel technique is given below.

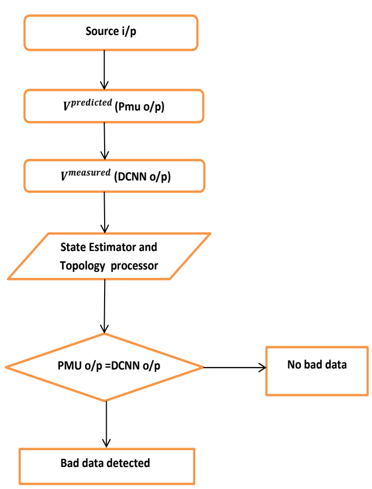


Figure 3: Flow Chart for bad data detection process

The Deep complex neural network produces the output of the predicted output for the voltage magnitude and the phase as $V^{measured}$ .The phasor quantities measured by the PMU were given as $V^{predicted}$. Bad data can also be identified using the topology processor. It detects the bad data that occurred due to the variations in the topology. Numerous measurements shown whenever an according to with of a PMU bus is adjusted by efficiency%, the influence of this measurement on the forecast of PMU bus voltage utilizing generates a prediction error that is consistently smaller than efficiency %. As a result, when the predicted bus voltage $V^{predicted}$ is compared to its corresponding observed equivalent $V^{measured}$ the greatest difference between the anticipated and measured bus voltages is seen.

An AC power distributor along with the Topology processor was incorporated for the betterment of the system. Thus by introducing the novel ideology of a Deep complex neural network, the topology processor incorporated with an AC estimator enhances the system by reducing the Disadvantages like complexity and increases efficiency. Thus the proposed approach increases the efficiency, accuracy, decreases the complexity. the bad data detection capability and detection range or the rate of bad data detection have been increased. The running time of the operation also decreased in the increase in performance of the proposed system.

The upcoming section explains the results obtained by MATLAB simulation and also the performance parameters were compared and analyzed.

4. Results and Discussions

This section provides a description of various implementation results and the performance analysis of our proposed model and also the comparison section to ensure enhancement of our proposed system.

4.1 Experimental Setup

This work has been implemented and the simulation of the system was then done using MATLAB with the following system specification and the simulation results are discussed below,

Platform : MATLAB
OS : Windows 8
Processor: Intel Core i5
RAM : 8GB RAM

The following diagram depicts the design of the proposed system. The Simulated design depicts the process carried over. Initially the voltage of three-phase V_{abc} , where the three phases are denoted as a,b,c respectively along with the phasor quantities like the magnitude of the voltage and also the phase of the voltage was obtained per unit (PU). Here the Phasor Measurement Unit (PMU) designed is based on phase locked loop-based positive –sequence. A PLL is a closed-loop system with a control mechanism to reduce any phase error that may occur.

Then the Deep Complex Neural System incorporated with the topology processor and the SE (State Estimator) performs the required function to produce the required results. Finally, the Bad data has been detected from the outputs obtained.

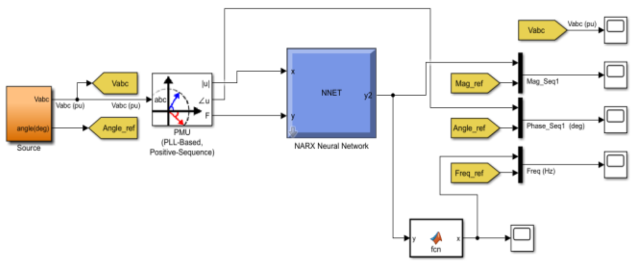


Figure 4: Simulated design for bad data detection

The Simulated design depicts the process carried over. Initially the voltage of three-phase V_{abc} , where the three phases are denoted as a,b,c respectively along with the phasor quantities like the magnitude of the voltage and also the phase of the voltage was obtained per unit (PU). Here the Phasor Measurement Unit (PMU) designed is based on Phase Locked Loop-based positive –sequence which is a closed-loop system with a control mechanism to reduce any phase error that occurs. Then the Deep Complex Neural System incorporated with the topology processor and the SE (State Estimator) performs the required function to produce the required results. Finally, the Bad data has been detected from the outputs obtained. The next diagram deals with the intrinsic functioning that happens in the proposed system.

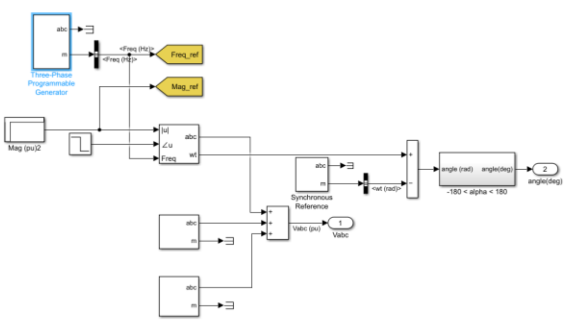


Figure 5: Simulated Design of Source

Figure 5 shows the internal functioning of the source. From the source, only the three-phase voltage along with the phasor quantity such as the voltage magnitude, phasor angle in degrees and also the frequency in hertz can be derived.

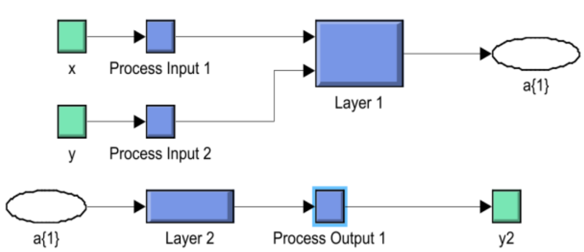


Figure 6: Internal Function of Deep Complex Neural Network

The output from the PMU, the voltage magnitude and the phase were given to the DCNN. As we already know that the DCNN consists of a hidden layer and they perform some functions so that the output is obtained from the other side as y2 depicted in figure 6.

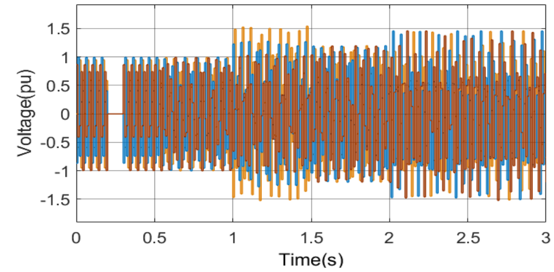


Figure 7: Output of Three Phase voltage

Three-phase voltage V_{abc} is initially received from the source input power grid. So finally the output obtained is also three-phase voltage.The output voltage obtained is maximum at time sequence 1s to 1.5s . The graph shows the final output V_{abc} .The three phases are differentiated by various colours in figure 7.

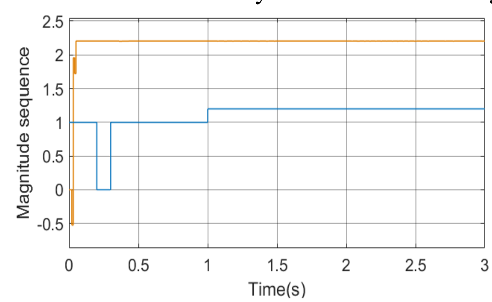


Figure 8: Simulated Output of Magnitude

The graphical representation in figure 8 has been drawn concerning time in seconds. This depicts both the active and the reactive magnitude sequence, where active represents the used magnitude reactive represents the unused magnitude. The active magnitude range reaches a maximum of 2.25 V and constant throughout the graph figure 8.

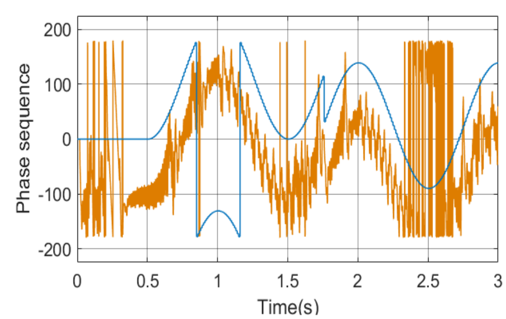


Figure 9: Simulated out of phase sequence in bad data detection

Graph in figure 9 depicts the simulated output of the phase /angle in degree obtained finally. Here also both the reactive, as well as the nonreactive angles, are shown in different colours. In figure 9 range of the phase sequence for both reactive and nonreactive angles reaches the maximum 180 .

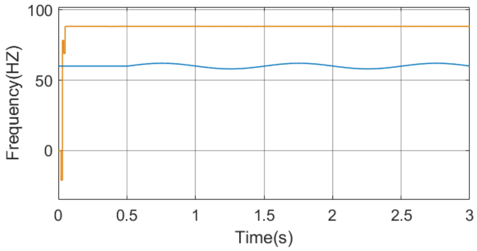


Figure 10: Simulated output of Frequency in bad data detection

Graph figure 10 depicts the simulated output of the frequency in hertz. Here both the reactive, as well as nonreactive frequencies were differentiated for the evaluation purpose. In our proposed system , Weight normalization have being incorporated into to the deeply complex neural network as a result of the integration of recurrent timestamps for monitoring voltage, magnitude, and phase angle, which improve model training efficiency even more.Thus the simulated output obtained shows better performance due to the AC state estimator and the Deep complex neural network in the proposed methodology .

4.2 Comparative Analysis

The comparative analysis provides better performance parameters when compared to the existing methods such as SVR, BP Neural Network, Spectral Clustering (SC), Ensemble Method(EM) and Density-Based Clustering (DBSCAN) [29].

In the following analysis, the parameters such as the Accuracy in percentage, Bad data Detection capability, Bad Data Detection range in terms of the deviation of phase angle, Running time in terms of time window as well as the data points were compared and the comparison graphs are given in the corresponding order.

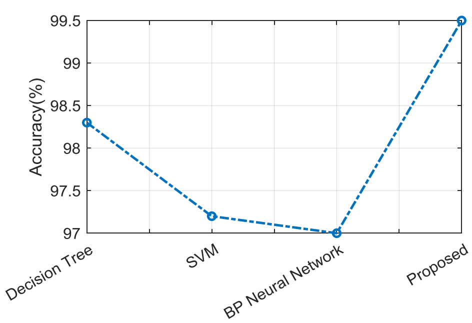


Figure 11: Accuracy Comparision

The Novel proposed technique using a Deep Complex neural network provides higher performance when compared to the previously existing techniques such as Decision Tree, SVM, BP Neural Technique has been highlighted in figure 11

Sl.No	Techniques	Accuracy(%)
1	BP Neural Technique	97%
2	Support Vector Machine	97.2%
3	Decision Tree	98.4%
4	Deep Neural Technique	99.5%

The Comparision of the detection capability of the bad data occurrence by the existing method with the proposed system is systematically represented utilizing Graphical manner in figure 12

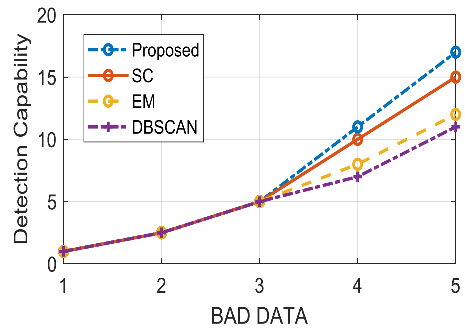


Figure 12: Comparison of Bad data detection Capability

Considering the maximum ratio of detection capability is 20 %. This graph shows that when the bad data detection ratio is higher than 11% the DBSCAN cannot detect completely. When the ratio reaches above 12% EM cannot detect the bad data. when it reaches above 15% also the spectral clustering won't detect it completely. But the proposed system shows betterment by detecting the bad data that occurred above the ratio level of about 18 %. Thus our novel approach produces better results in the detection capability.

The next parameter analysed for the comparison is the detection range according to the deviation angle. The bad data also occurs due to the phase angle deviation based on the phase angle deviation the bad data detection range is observed. Here considering the maximum deviation phase angle is 5. The graphical representation of the detection range in terms of deviation phase angle is given below.

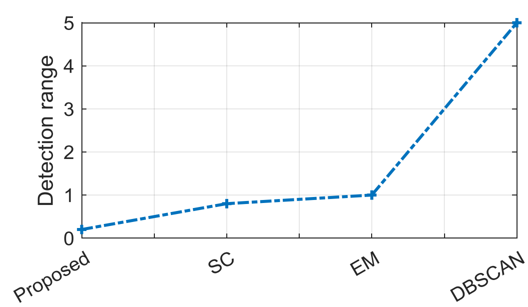


Figure 12: Comparison of detection range

The DBSCAN will not detect any bad data when the below deviation angle of 5. EM will not detect any bad data when the deviation angle ranges below 1. The spectral clustering method will not detect any bad data when the deviation angle ranges below 0.8. In our proposed system, the bad data can be detected from 0.2 deviations of phase angle to the maximum of 5 . Hence it is again proved that our proposed system shows more improvement than the old methodologies.

The next parameter compared is the Running time. The running time is calculated in seconds. Hence we are using Weight normalization the parameter called the running time is reduced for our proposed system. This is compared for both the time window as well as the data points. The graphical representation of the running time in terms of the time window and the data points were compared and analyzed in figure 13. A decrease in running time increases the efficiency of the system.

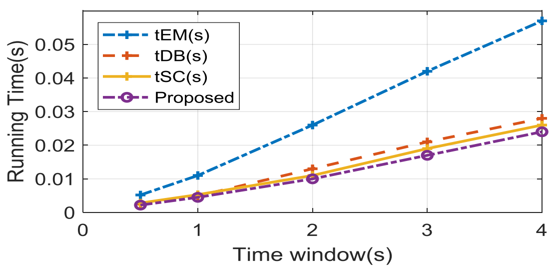


Figure 13: Comparison of Running time with Time windows

Based on the time windows the data points are calculated. So for time window 1, the data points appeared 50. For Time window 2 the data points given are 100. Thus increase in the time window increases the Datapoint. The Running time of the system in the old existing techniques such as the EM, SC, DB were much higher for the data points analyzed. The same data points, as well as the time windows, are analyzed for our proposed system of Novel bad detection techniques. The Running time of the system is lower when compared.

The running time for the EM technique is about 0.05 seconds. Running time for DB is 0.029 seconds and for SC technique is about 0.028 seconds. But the proposed system produces a lesser running time of 0.024 seconds which is comparatively lesser than the previously existing technique. The graphical representation of running time for both the time window and the data points were shown as a graphical representation in figure 13 and 14.

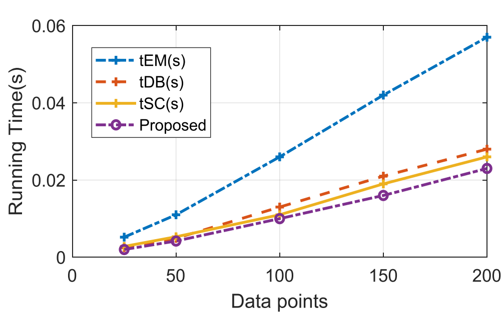


Figure 14: Comparison of Running time along with Datapoints

Thus the simulated output for the robust Bad data detection technique was explained along with the functional diagram of the source and Deep complex neural network. Also, the simulated analysis and the output for the voltage of three-phase (Vabc), Magnitude sequence of the voltage (|u|), Phase angle of the voltage, Frequency in Hertz were derived.

Then the comparative analysis of the various parameters is also analyzed and depicted in the corresponding figures.

5. Conclusion

The Proposed Power Data Quality improvement through PMU Bad Data Detection Based on Deep Complex Network approach was tested effectively and its superiority over other models was determined. The current strategy provides better accuracy of 99.5% over other existing models. Also, the complexity of the basic system has been reduced by introducing the Deep complex neural network also the detection of bad data due to the phase angle deviation is also achieved by the novel approach. Lesser training time is also achieved by using weight normalization. It also shows betterment by detecting the bad data that occurred above the ratio level of about 18 % of 20% . The running time for the execution of 200 data points is reduced to 0.023 s. The bad data can be detected from 0.2 deviations of phase angle to the maximum of 5. Due to the implemented Novel approaches, the efficiency of our system increased with higher data detection rate when compared with the other existing systems.

References

[1]. O.I. Abiodun, E.O. Abiodun, M. Alawida, R.S. Alkhawaldeh, H. Arshad, “A Review on the Security of the Internet of Things: Challenges and Solutions,” Wireless Personal Communications, 2021, pp. 1-35.

[2]. Jia, Ke, et al. "Transient high-frequency impedance comparison-based protection for flexible DC distribution systems." IEEE Transactions on Smart Grid, vol. 11, no. 1 pp. 323-333, 2019.

[3]. S. Shankar, K.B. Yadav, A. Priyadarshi, and V. Rathore, “Study of phasor measurement unit and its applications,” In Recent Advances in Power Systems, 2021, pp. 247-257). Springer, Singapore.

[4]. Usman, Muhammad Usama, and M. Omar Faruque, "Applications of synchrophasor technologies in power systems,” Journal of Modern Power Systems and Clean Energy, vol. 7, no. 2, pp. 211-226, 2019.

[5]. Jia, Ke, et al., "Sparse voltage measurement-based fault location using intelligent electronic devices,” IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 48-60, 2019.

[6]. Liu, Hao, et al. "Data-Driven Subsynchronous Oscillation Identification Using Field Synchrophasor Measurements." IEEE Transactions on Power Delivery, 2021.

[7]. D. Ghosh, “Novel trends in resilience assessment of a distribution system using synchrophasor application: A literature review,” International Transactions on Electrical Energy Systems, vol. 31, no. 8, pp. e12934, 2021.

[8]. Mian, Ishaq, "Probability Estimation Models to Predict Risk Occurrence in Smart Grid Projects." PhD diss., The George Washington University, 2021.

[9]. Li, Jian, Chaowei Sun, and Qingyu Su, "Analysis of cascading failures of power cyber-physical systems considering false data injection attacks," Global Energy Interconnection, vol. 4, no. 2, pp. 204-213, 2021.
[10]. C. Pei, Y. Xiao, W. Liang, X. Han, "A Deviation-Based Detection Method Against False Data Injection Attacks in Smart Grid," IEEE Access, vol. 12, no. 9, pp. 15499-509, 2021.
[11]. X. Luo, M. Pajic, and M.M. Zavlanos, "An optimal graph-search method for secure state estimation," Automatica, vol. 123, p.109323, 2021.
[12]. S. Hopkins, E. Kalaimannan, C.S. John, "Sub-Erroneous Outlier Detection of Cyber Attacks in a Smart Grid State Estimation System," In2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020, pp. 0447-0454. IEEE.
[13]. Pagnier, Laurent, and Michael Chertkov, "Embedding Power Flow into Machine Learning for Parameter and State Estimation," arXiv preprint arXiv:2103.14251, 2021.
[14]. A. R. Kulkarni, & M. S. Ballal, "Synergism of synchrophasor measurements and data analytics for enhancing situational awareness of power grid," Computers & Electrical Engineering, vol. 93, pp. 107231, 2021.
[15]. Lu, Jiyong; Wang, Weizhen, Li, Li, Guo, Yanping, "Unscented Kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks," Asian Journal of Control, 2019, asjc.2262–.
[16]. Gu, Yingzhong, Zhe Yu, Ruisheng Diao, and Di Shi, "Doubly-fed Deep Learning Method for Bad Data Identification in Linear State Estimation," Journal of Modern Power Systems and Clean Energy, vol. 8, no. 6, pp. 1140-1150, 2020.
[17]. Shereen, Ezzeldin, et al., "Feasibility of time-synchronization attacks against PMU-based state estimation," IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 6, pp. 3412-3427, 2019.
[18]. S. V. S. Chauhan, & G. X. Gao, "Synchrophasor Data Under GPS Spoofing: Attack Detection and Mitigation Using Residuals," IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3415–3424, 2021.
[19]. Sundararajan, Aditya, et al., "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," Journal of Modern Power Systems and Clean Energy, vol. 7, no. 3, pp. 449-467, 2019.
[20]. M. Dorier, G. Frigo, A. Abur, M. Paolone, "Leverage Point Identification Method for LAV-Based State Estimation," IEEE Transactions on Instrumentation and Measurement, vol. 70,pp.1-0, 2021.
[21]. Aljohani, Nader, and Arturo Bretas, "A Bi-level model for detecting and correcting parameter cyber-attacks in power system state estimation," Applied Sciences, vol. 11, no. 14, pp. 6540, 2021.
[22]. B. Li, R. Lu, & G. Xiao, "Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems," Springer, 2020.
[23]. L. Kumar, & P. K. Kherdikar, "An overview of different static state estimation techniques with bad data detection, identification and elimination in power system," International Journal of Ambient Energy, pp. 1-5, 2021.
[24]. Khare, Gaurav, Mohapatra, Abheejeet, S.N. Singh, "A Real-Time Approach for Detection and Correction of False Data in PMU Measurements," Electric Power Systems Research, vol. 191, pp. 106866–,2021.
[25]. M. Shahraeini, A. Alvandi, & S. Khormali, "Behavior Analysis of Random Power Graphs for Optimal PMU Placement in Smart Grids," 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2020.
[26]. A. L. Amutha, R. Annie Uthra, J. Preetha Roselyn, & R. Golda Brunet, "Anomaly detection in multivariate streaming PMU data using density estimation technique in wide area monitoring system," Expert Systems with Applications, vol. 175, pp. 114865, 2021.
[27]. A. Ahmed, K. S. Sajan, A. Srivastava, & Y. Wu, "Anomaly Detection, Localization and Classification Using Drifting Synchrophasor Data Streams," IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3570–3580, 2021.
[28]. Nawaz, Rehan, Rabbaya Akhtar, Muhammad Awais Shahid, Ijaz Mansoor Qureshi, and Muhammad Habib Mahmood, "Machine learning based false data injection in smart grid," International Journal of Electrical Power & Energy Systems, vol. 130, pp. 106819, 2021.
[29]. Yang, Zhiwei, et al., "Bad data detection algorithm for PMU based on spectral clustering," Journal of Modern Power Systems and Clean Energy, vol. 8, no. 3, pp. 473-483, 2020.
[30]. Jovicic, Aleksandar, and Gabriela Hug, "Linear state estimation and bad data detection for power systems with RTU and PMU measurements," IET Generation, Transmission & Distribution, vol. 14, no. 23, pp. 5675-5684, 2020.