Available online at www.sciencedirect.com

ScienceDirect

Energy Reports 8 (2022) 919–930

www.elsevier.com/locate/egyr

2022 The 5th International Conference on Renewable Energy and Environment Engineering (REEE 2022), 24–26 August, 2022, Brest, France

Deep learning-based identification of false data injection attacks on modern smart grids

Debottam Mukherjee[a], Samrat Chakraborty[b], Almoataz Y. Abdelaziz[c], Adel El-Shahat[d,*]

[a] *Department of Electrical Engineering, Indian Institute of Technology (BHU), Varanasi 221005, India*
[b] *Department of Electrical Engineering, National Institute of Technology Arunachal Pradesh, Jote 791113, India*
[c] *Faculty of Engineering and Technology, Future University in Egypt, Cairo, Egypt*
[d] *Energy Technology Program, School of Engineering, Purdue University, West Lafayette, IN 47907, USA*

Received 6 October 2022; accepted 10 October 2022
Available online 31 October 2022

Abstract

With the rapid adoption of renewables within the conventional power grid, the need of real-time monitoring is inevitable. State estimation algorithms play a significant role in defining the current operating scenario of the grid. False data injection attack (FDIA) has posed a serious threat to such kind of estimation strategies as adopted by modern grid operators by injecting malicious data within the obtained measurements. Real-time detection of such class of attacks enhances grid resiliency along with ensuring a secured grid operation. This work presents a novel real-time FDIA identification scheme using a deep learning based state forecasting model followed with a novel intrusion detection technique using the error covariance matrix. The proposed deep learning architecture with its optimum class of hyper-parameters demonstrates a scalable, real-time, effective state forecasting approach with minimal error margin. The developed intrusion detection algorithm defined on the basis of the error covariance matrix furnishes an effective real-time attack detection scheme within the obtained measurements with high accuracy. The aforementioned propositions are validated on the standard IEEE 14-bus test bench.

Peer-review under responsibility of the scientific committee of the 5th International Conference on Renewable Energy and Environment Engineering, REEE, 2022.

Keywords: False data injection attack; Intrusion detection; Smart grid; State estimation

1. Introduction

With a high penetration of inverter based renewable energy resources along with a large scale adoption of plug in electric vehicles within the conventional power sector, the control centers need to assess the current operating scenario based on the set of acquired measurements at supervisory control and data acquisition (SCADA) system in real-time. A rapid adoption of industrial internet of things (IIOT) technology within the power network although leads to a higher reliability, still it imposes an inherent vulnerability as it is prone to cyber-attacks. The obtained

[*] Corresponding author.
E-mail address: asayedah@purdue.edu (A. El-Shahat).

https://doi.org/10.1016/j.egyr.2022.10.270

Peer-review under responsibility of the scientific committee of the 5th International Conference on Renewable Energy and Environment Engineering, REEE, 2022.

measurements as retrieved from the remote terminal units (RTUs), phasor measurement units (PMUs), local phasor data concentrators (PDCs) lead to an efficient determination of the prevalent operating scenario of the power network with the aid of state estimation algorithms residing within the energy management systems (EMSs) in the control center [1,2].

Recently, with an effective undermining of the critical vulnerabilities of the RTU and IIOT devices by the intruders, an advanced genre of cyber-attack such as the false data injection attack (FDIA) has been presented [3], which can effectively elude the bad data detector (BDD) as employed by the operators in the control center of the power network, hence developing a set of falsified state estimates. A polynomial time complexity attack vector formulation algorithm undertaking an optimization problem which incorporates the impact of attack along with its detection probability using the conventional BDD may lead to critical operating conditions of the grid [4]. Furthermore, such an attack vector formulation scheme may also lead to transmission line congestion [5], modification of dynamic pricing in electricity market [6] and control signals as developed by the modern grid operators [7,8]. Attacks against the distribution sector like consumers, feeders, substations etc. have also been demonstrated which leads to a significant socio-economic impact on the power sector [9]. A set of falsified state estimates may eventually develop mal-operations of the smart grid, hence a new concept of holistic resilience cycle has been recently demonstrated which is primarily introduced to enhance the cyber–physical security of the grid [10]. With access to smart meters of the consumers, such attacks may target the data integrity of energy supply and demand and is capable of successfully modifying the measurements [11,12]. Attacking the transmission sector with such kind of attacks by targeting the optimal power flow module within the EMS in the control center may also develop overloading of the transmission lines with a possibility of physical damage and power outage [13]. In case of microgrids, FDIAs may effectively lead to power losses with a significant disruption in dynamic microgrid partitioning [11,14,15]. The recent studies in this domain portray that most of the attack vectors formulated on the basis of the full column space of the mapping matrix can efficaciously evade the residue test as utilized by the traditional BDD. With access to measurements and topology information of the grid, a low-rank subspace based data-driven attack vector formulation using reduced order and full order singular value decomposition technique has recently demonstrated a significant impact [16–18]. It can be seen from [19–22] that the intruder is capable of developing a stealthy attack vector with limited topology information of the grid.

Determining the presence of such genre of attacks within the raw measurements at SCADA is a potential research prospect. The primary defense strategies adopted in practice can be categorized into two different classes as physical defending policy and data-driven detection schemes. In case of physical defending policy, the grid operator defines a critical set of RTUs and sensors on the basis of which the full rank topology matrix can be formulated, hence ensuring grid observability under all circumstances [23,24]. With an optimal allocation of data diodes and PMUs, the set of acquired measurements can be protected from such class of attacks, hence improving the resiliency of the state estimation algorithms [25–27]. The primary drawback of such an approach is the high cost and minimal possibility of reconfiguration and reallocation of such devices followed by selection of the critical set of measurements needed to be protected. Furthermore, there is a drop in measurement redundancy, hence an optimal solution of the estimation model cannot be guaranteed under all operating conditions [28]. Recently, with the implementation of graph signal processing and graph Fourier transform, detection of undetectable stealthy FDIA with high accuracy has been achieved [29,30]. Tree pruning based approximation algorithms have also defined a scalable attack detection policy [31]. Anomaly detection approaches undertaking the predicted and the estimated set of operating states at SCADA have also defined a prospective FDIA detection scheme [32–36].

An efficient strategy to determine the locations of intrusions of such attacks along with their presence detection within the set of available measurements at SCADA has been also recently furnished [37,38]. Such schemes incorporate advanced deep learning structures which work as multilabel classifiers and are capable of detecting the locations of intrusions of attack with high accuracy. With a rapid advancement in machine learning approaches, an effective state forecasting scheme has been showcased [39,40]. Such trained state forecasting models demonstrate a minimal root mean squared error (RMSE), mean squared error (MSE) and mean absolute error (MAE) index. This work demonstrates an accurate real-time presence detection of such attacks within the acquired measurements by deploying deep learning models for an accurate state forecasting followed by an effective anomaly detection scheme within the estimated states using the error covariance matrix. The grid operator reveals the existence of an attack within the set of available measurements at SCADA when the rate of change of the eigen values of the error covariance matrix overshoots a predefined threshold. This work demonstrates an effective deployment of a scalable, robust, nonlinear deep learning model which demonstrates a superior state forecasting scheme with minimum indices like RMSE, MAE and MSE. The key proposals of this work are defined as follows:

- With an effective tuning of model hyper-parameters of the developed deep learning structure, a set of minimal error indices have been achieved. A comprehensive contrast among two non-identical deep learning models followed by a conventional machine learning model like support vector machine (SVM) and a statistical forecasting model like autoregressive integrated moving average (ARIMA) has been undertaken in this work.
- With incorporation of noise within the available measurements, the developed deep learning model furnishes a resilient operation with a minimum variation in the error indices, hence leading to a minimal variation in the attack detection probability.
- The developed anomaly detection algorithm demonstrates a superior, real-time, robust FDIA identification scheme by tracking the rate of change of the eigen values of the error covariance matrix.
- As the proposed scheme does not demand any substantial adjustment of the traditional BDD, hence it demonstrates a cost-effective approach.

This work can be ordered as follows: Section 2 demonstrates briefly the nonlinear state estimation algorithm as deployed in the modern control centers followed by formulation of an undetectable stealthy attack vector which can efficiently bypass the statistical residue test as adopted by the BDD. Section 3 extensively elaborates the proposed scalable, nonlinear deep learning model adopted for prediction of the estimated operating states of the power network followed by the proposed anomaly detection algorithm developed on the basis of the error covariance matrix. Section 4 furnishes the obtained results, while Section 5 concludes this research with the future prospects and potential outcomes.

2. State estimation and FDIA

Operators at the control center adopt state estimation algorithms to define the critical grid operations like load forecasting, economic load dispatch etc [1]. The available measurements at SCADA are filtered through the BDDs to cater the quality and integrity of the measurements followed by discarding of the bad data due to noise within communication networks, meter malfunctioning etc. Unlike most of the works [3,16,17] which adopt a linear state estimation model, this work has undertaken a nonlinear state estimation technique which can be demonstrated as:

$$z = h(x) + e_1 \tag{1}$$

where, $z \in \mathfrak{R}^m$ denotes the available measurements as derived from the BDDs. $x \in \mathfrak{R}^n$ furnishes the set of operating states while $e_1 \in \mathfrak{R}^m$ represents the error vector for the estimation model. $h(.)$ denotes a nonlinear function which maps the set of acquired measurements with the operating states of the grid. To estimate the set of operating states using the nonlinear state estimation model as shown in (1), a flat start approach as shown in (2) has been adopted.

$$x[0] = [0\,0\ldots 1\,1]^T \tag{2}$$

All the bus voltage magnitudes are supposed to be 1 p.u. with their corresponding phase angles being 0 at start (as shown in 2). Using the flat start approach, an iterative honest Gauss Newton (HGN) technique is undertaken to determine the set of estimated states as shown in Algorithm 1 where the Jacobian matrix $J(J \in \mathfrak{R}^{m\times n})$ is reformulated at every single iteration. It can be seen from algorithm 1 that the set of estimated operating states can be denoted by $\hat{x}(\hat{x} \in \mathfrak{R}^n)$, while ϵ is defined in the range of 10^{-7}. The BDD present within the EMS module in SCADA undertakes the statistical residue test as shown:

$$r = \|z - h(\hat{x})\|_2 \leq \tau \tag{3}$$

where, τ depends on the degrees of freedom $(m - n)$ of the over determined system. As the acquired measurements have sufficient redundancy in them, hence measurements showing higher residues than τ are successfully discarded as a potential bad data.

Algorithm 1: Nonlinear HGN State Estimation Algorithm

```
Input: $x[0] \in \Re^{n}$: Initial vector of state variables undertaken for flat
        start approach; $J[0] \in \Re^{m \times n}$: Jacobian matrix during
        initialization formulated from $x[0]$ and $z$; $z \in \Re^{m}$: Input
        measurement vector as received from the BDD; $h(.) \in \Re^{m}$:
        Nonlinear function mapping the acquired measurements with
        the operating states; $W \in \Re^{m \times m}$: Weight matrix of the
        respective RTUs and sensors
Output: $\hat{x} \in \Re^{n}$: Estimated operating states
Initialization $s = 0$, Formulate the convergence criteria: $\epsilon$
while $||x[s+1] - x[s]||_2 \leq \epsilon$ do
    Compute $\Delta x[s]$ as follows:
    $\Delta x[s] = (J[s]^T W J[s])^{-1} J[s]^T W (z - h(x[s]))$
    $x[s+1] = x[s] + \Delta x[s]$
    Update $J[s+1]$ based on $x[s+1]$ and $z$ : $J[s+1] = f(x[s+1], z)$
end while
$\hat{x} = x[s+1]$;            // Estimated set of operating states
return $\hat{x} \in \Re^{n}$;        // termination of pseudo code
```

2.1. False data injection attack

The sole intention of such kind of an attack is to bypass the residue test as adopted at the control centers by undermining the critical vulnerabilities of the RTUs and sensors. Such an advanced cyber-attack strategy on the modern grid leads to an altered set of state estimates from a corrupted set of acquired measurements. This work demonstrates an undetectable stealthy attack vector development scheme for the nonlinear state estimation algorithm as shown:

$$a_1 = h\left(\hat{x}_{a_1}\right) - h\left(\hat{x}\right); \quad \hat{x}_{a_1} = \hat{x} + c'; \quad z_{a_1} = z + a_1 \tag{4}$$

where, $a_1 (a_1 \in \Re^m)$ furnishes the attack vector injected into the set of acquired measurements z to furnish a corrupted set of measurements $z_{a_1} (z_{a_1} \in \Re^m)$, hence developing a falsified set of estimated states $\hat{x}_{a_1} (\hat{x}_{a_1} \in \Re^n)$. The statistical residue test as undertaken by the BDD under the aforesaid circumstances can be seen as:

$$\begin{aligned} r_{a_1} &= \|z_{a_1} - h(\hat{x}_{a_1})\|_2 \\ &= \|z + a_1 - h\left(\hat{x}_{a_1}\right) + h\left(\hat{x}\right) - h\left(\hat{x}\right)\|_2 \\ &= \|z - h\left(\hat{x}\right)\|_2 = r \end{aligned} \tag{5}$$

It can be seen from (4) and (5) that the developed attack vector can successfully bypass the residue test, hence leading to critical operating scenarios of the power sector.

3. Proposed forecasting policy

In the recent past, both an effective and an accurate performance for regression-based analysis has been showcased by deep learning models. Such kind of a data-driven predictive policy has demonstrated a nominal error during prediction [41–43]. The current research considers RMSE, MSE and MAE as the performance parameters that can be defined by:

$$RMSE = \sqrt{\sum_{a''=1}^{b''} \frac{(f''_{a''} - s''_{a''})^2}{b''}} \tag{6}$$

$$MSE = \sum_{a''=1}^{b''} \frac{(f''_{a''} - s''_{a''})^2}{b''} \tag{7}$$

$$MAE = \sum_{a''=1}^{b''} \frac{|f''_{a''} - s''_{a''}|}{b''} \tag{8}$$

Here, the predicted operating states are demarcated by f'' and the actual operating states are demarcated by s''. The total number of samples for prediction is b''. With an effective hyper-parameter optimization, the proposed neural network model under steady state scenario of the power network can efficiently predict the estimated states with the least performance parameters (RMSE, MSE and MAE). In this research, the suggested robust, nonlinear LSTM structure shows an improved forecasting of the operating states when compared to existing SOA (state-of-the-art) state forecasting models viz. multi-layered perception (MLP), SVM and ARIMA [33–36].

3.1. Proposed state forecasting scheme

LSTM is a special structure of recurrent neural networks (RNNs) which helps to learn complicated temporal patterns that are present within the training dataset. These special types of RNNs are capable of intrinsically retaining such information over a distinct time-step. Therefore, LSTM bears the ability of studying, preserving and eliminating data from the cells of the memory via adjusting three distinguished controllable gates namely forget $g_1''(t)$, input $j_1''(t)$, and output $p_1''(t)$ gate respectively. Fig. 1 indicates a single cell structure of an LSTM module while the proposed LSTM model is shown as per Fig. 2.

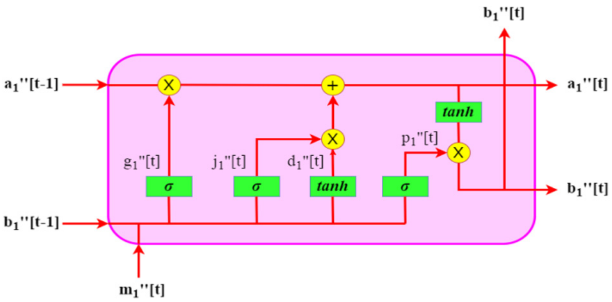

Fig. 1. The single cell structure of LSTM.

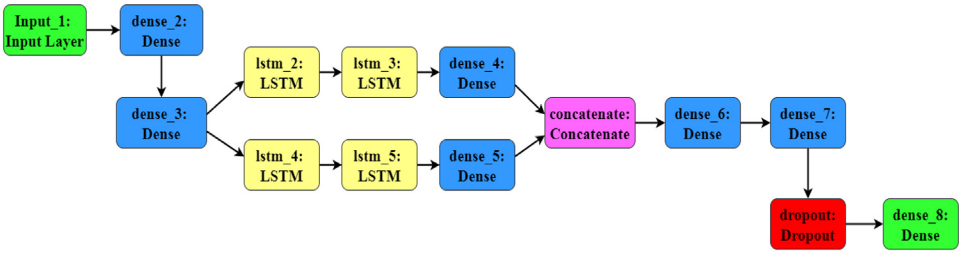

Fig. 2. The proposed LSTM model.

The acceptance or refusal of data in binary form (i.e. 0 or 1) pertaining to the cells current state depends on $g_1''(t)$, the forget gate as signified by (9). In the LSTM modules, sigmoid (σ) activation has been adopted. $j_1''(t)$ signifies the input gate of the LSTM module as shown in (11). To update the current cell state, a binary decision (i.e. 0 or 1) is generally adopted by $j_1''(t)$ (input gate). For the LSTM module, the updated cell state is demarcated by $a_1''(t)$ while the new participant is $d_1''(t)$. The accumulated data is discharged towards the succeeding neurons as decided by the output gate $p_1''(t)$, as shown in (13). Here, the weights are indicated by $w_{1(.)}''$, the output is indicated by $b_1''(t)$, the input is indicated by $m_1''(t)$ and the biases are indicated by $b_{1(.)}'''$, as depicted in (9)–(14). The operation for concatenation is represented by [., .].

$$g_1''(t) = sig(w''_{1_{g_1''}}\left[b_1''(t-1), m_1''(t)\right] + b'''_{1_{g_1''}}) \tag{9}$$

$$a_1''(t) = \left[g_1''(t) \times a_1''(t-1)\right] + \left[j_1''(t) \times d_1''(t)\right] \tag{10}$$

$$j_1''(t) = sig(w''_{1_{j_1''}}\left[b_1''(t-1), m_1''(t)\right] + b'''_{1\,j_1''}) \tag{11}$$

$$d_1''(t) = tanh(w''_{1_{d_1''}}\left[b_1''(t-1), m_1''(t)\right] + b'''_{1_{d_1''}}) \tag{12}$$

$$p_1''(t) = sig(w''_{1_{p_1''}}\left[b_1''(t-1), m_1''(t)\right] + b'''_{1_{p_1''}}) \tag{13}$$

$$b_1''(t) = p_1''(t) \times tanh(a_1''(t)) \tag{14}$$

Fig. 2 indicates that the recommended LSTM model has overall eight number of hidden layers together with one output layer and one input layer. It can be seen that at the second hidden layer, the model is split with sub-hidden layers. The sub-hidden layers incorporate LSTM structures with dense neural networks to enhance the state forecasting performance. Such nonlinear models with sub-hidden layers are found to demonstrate a better forecasting strategy. Ultimately, all the hidden sub-layers are combined into a common layer known as the concatenation layer. Two dense layers succeed the concatenation layer followed by the output layer. Drop-out regularization has been effectively adopted in order to avoid the over-fitting of the model. The recommended nonlinear model has been fed by ReLU activation function at each and every layer that can be stated by (15).

$$y''_{1_{i_1'}} = ReLU(w''_{1_{i_1'}} k'_{1_{i_1'}} + b'''_{1_{i_1'}}) \tag{15}$$

In the above equation, for i_1'th layer the predicted feature set is $y''_{1_{i_1'}}$ and the input feature is $k'_{1_{i_1'}}$. The other parameters for that particular layer are: weight ($w''_{1_{i_1'}}$) and the bias ($b'''_{1_{i_1'}}$) respectively. The output for the LSTM layer i.e. $b_1''(t)$ of the proposed nonlinear model is fed directly into the next dense layer which has ReLU as an activation function. The output layer of the nonlinear structure encompasses a ReLU activation function as per (15). The recommended model has been trained with 500 iterations (epochs) using adam optimizer. The preliminary learning-rate of the model is 0.001. For the efficient training of the proposed model, both the historical and the estimated set of the operating states are considered together which constitutes the dataset. Now, this dataset is bifurcated in the ratio of 7:3 where 70% of the data (training dataset) is fed as input to the nonlinear model, MLP, SVM and ARIMA whereas the rest 30% is employed for the model's effective testing. 10% of the data for training is used to validate the model's performance.

3.2. Recommended detection scheme for FDIA

With effectual training of the models, a superior policy to forecast the states with minimum error indices can be showcased. The developed real-time FDIA detection scheme based on the error covariance matrix can be seen as per Fig. 3. The proposed abnormality recognition algorithm undertakes the error vector developed due to the estimated and the forecasted operating states at SCADA as shown:

$$e(t) = \hat{x}_{for}(t) - \hat{x}_{est}(t) \tag{16}$$

where, $\hat{x}_{for}(t) \in \Re^n$ represents the forecasted set of estimated states as derived from the scalable, nonlinear neural network architecture and $\hat{x}_{est}(t) \in \Re^n$ denotes the estimated states for the existing time step t as retrieved from the

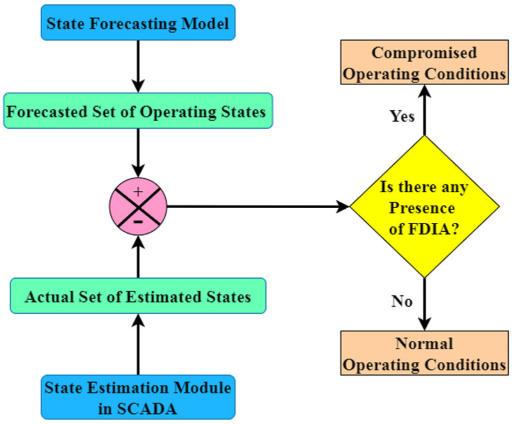
State Forecasting Model
Forecasted Set of Operating States
+
-
Actual Set of Estimated States
State Estimation Module in SCADA
Compromised Operating Conditions
Yes
Is there any Presence of FDIA?
No
Normal Operating Conditions

Fig. 3. Proposed FDIA detection scheme.

state estimation algorithm present inside the EMS component in SCADA. $e(t) \in \Re^n$ represents the error vector. The primary objective of the anomaly detection scheme lies in identifying the rate of change of the eigen values of the error covariance matrix as shown:

$$\frac{d\lambda}{dt} = x_1^T(t)\,\frac{dE(t)}{dt}x_1(t) \tag{17}$$

$$\text{where, } \frac{dE}{dt} \approx \frac{E(t) - E(t-\delta t)}{\delta t} \tag{18}$$

where, $x_1(t) \in \Re^n$ represents the eigen vector for the error covariance matrix $E(t) \in \Re^{n\times n}$ developed during the current sampling time t. As $E(t)$ and $E(t)^T$ are positive definite symmetric covariance matrices, hence they have similar eigen values and eigen vectors. The rate of change of the eigen values between two successive time intervals t and $(t-\delta t)$ (for a very small δt) can be represented by (17) and (18) respectively. As SCADA samples the measurements at an order of a few hundred Hz, hence δt can be determined in the order of a few milliseconds. The proposed FDIA detection scheme undertaking the rate of change of the eigen values can be defined as:

$$\varepsilon = \begin{cases} 1 & d\lambda/dt > RMSE + \delta_1 \\ 0 & Otherwise \end{cases} \tag{19}$$

where, ε represents the detection criterion which is set to 1, hence denoting the existence of FDIA inside the acquired measurements if the rate of change of the eigen values ($\frac{d\lambda}{dt}$) for a particular time instant t overshoots a predefined threshold as shown in (19). δ_1 represents a very small positive numeric constant ($\approx 10^{-5}$) that depends on operator knowledge. Such kind of a parameter is intrinsically negligible as the nonlinear state forecasting model demonstrates an improved accuracy to forecast. The proof of (17) can be seen in Appendix.

4. Results

In this section, FDIA has been implemented as per Section 2 over the IEEE 14-bus test bench following an efficient detection. For the formulation of an attack, the attack vector has been primarily demarcated inside the unit ball ($\mathcal{L}_2$ norm). During training, RMSE is employed as the loss-function. Fig. 4 indicates the minimization of the loss-function for each and every epoch, hence showcasing an effectual tuning of the hyper-parameters of the developed model.

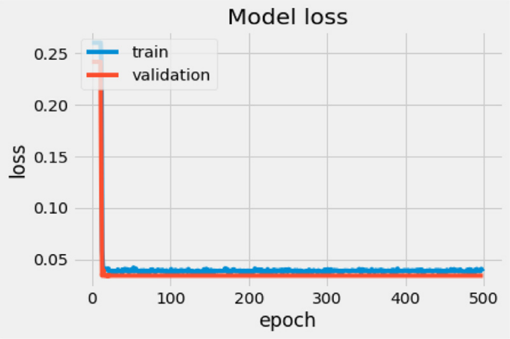

Fig. 4. Training loss and validation loss against each epoch for the developed model.

From Figs. 5–6 it can be concluded that the nonlinear LSTM model can efficiently predict the estimated states (voltage magnitude and their respective angles) efficiently with a forecasting range of about 200 samples. Besides, it is also noticed that the suggested nonlinear LSTM structure demonstrates a better forecasting for the operating estimated states (voltage magnitude along with angles) in comparison to the SOA forecasting schemes viz.: MLP, SVM and ARIMA [33–36].

Therefore, it is observed from Figs. 5–6 that the suggested nonlinear LSTM structure showcases an efficient forecasting of the estimated states i.e. voltage magnitudes and voltage angles up to nearly 7 time steps. Table 1 indicates that the suggested nonlinear LSTM structure has the minimal performance parameters (RMSE, MSE and

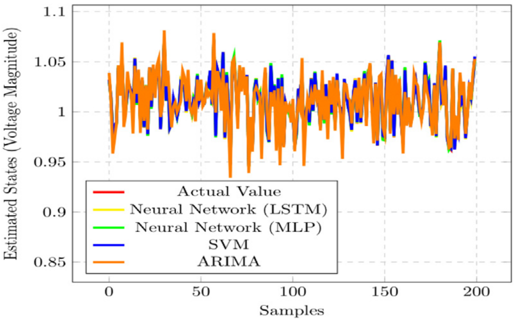

Fig. 5. Performance related to the voltage magnitudes (estimated) forecasting.

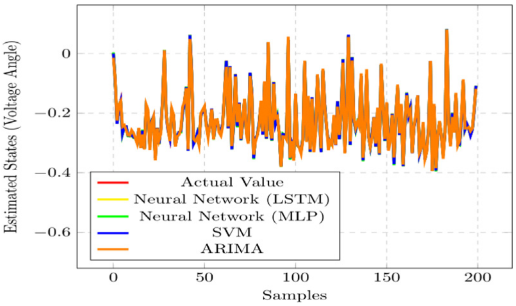

Fig. 6. Performance related to the voltage angles (estimated) forecasting.

Table 1. Comparison between performance index for different models for forecasting.

Models for forecasting	RMSE	MSE	MAE (%)
LSTM	0.000057	0.3249×10^{-8}	0.00872
MLP [33]	1.4221	2.0223	5.4886
SVM [33–36]	1.7103	2.9251	5.9612
ARIMA [33–36]	3.3245	11.0523	6.9221

MAE) in contrast to other advanced state forecasting schemes namely MLP, SVM and ARIMA hence promoting a superior state forecasting policy. In comparison to the nonlinear deep neural network model as shown in [33–36], the suggested robust nonlinear neural network model encompassing LSTM modules demonstrate the least performance parameters with a subsequent enhancement in prediction.

4.1. FDIA identification

The proposed scheme for detection of FDIA as described in Section 3.2 undertakes IEEE 14-bus as the test bench. From Fig. 7, it is noticed that the recommended FDIA identification policy can strategically detect the presence of attacks with accuracy higher than 95%. The developed FDIA detection strategy adopts a deterministic threshold over the estimated states. With the injection of attack vectors, a definitive deviation in the estimated states are observed. Operator reports a successful identification of an attack present inside the measurements when such aforesaid deviations as per (19) overshoot the deterministic threshold. Furthermore, it can be concluded from Fig. 7, that the proposed LSTM model detects the presence of FDIA with a probability of 95% for an attack vector having an $\mathcal{L}_2$ norm of strength equal to five times the unit ball in comparison to the nonlinear MLP model [33], whose detection probability is furnished as 91%. With a higher order FDIA as shown in Fig. 7, a higher FDIA identification has been achieved. The primary reason for such an enhanced detection probability can be outlined as that with a lower order attack vector formulation, noise within the raw measurements due to communication channels, meter failure etc. cannot be effectively distinguished from attack. A variation in the FDIA identification probability due

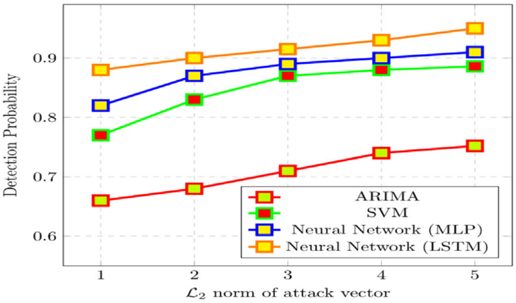

Fig. 7. FDIA identification probability with different models.

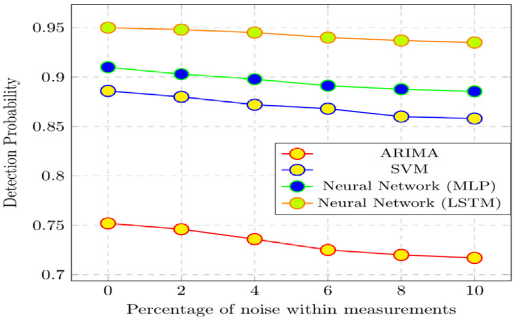

Fig. 8. FDIA identification probability with different models under varying measurement noise.

to presence of noise within the measurements can be seen in Fig. 8. Here, Gaussian noise has been considered with standard deviation and mean of 1 and 0 respectively. It is observed that with an increase in noise, the detection probability of FDIA diminishes. It can also be concluded from Fig. 8 that the developed nonlinear LSTM structure demonstrates a minimum deviation in the FDIA detection probability under varying noise margins, hence can be seen as a robust FDIA detector.

4.2. Computational efficacy

The real-time performance of the proposed robust, nonlinear LSTM model is presented in this sub-section. The ARIMA model demonstrates the lowest time for training and testing together with lower performance parameters, hence indicating an inferior forecasting of the estimated operating states of the grid. Thus ARIMA develops a slackly bounded identification criterion for FDIA. Although, it showcases the lowest detection accuracy with respect to the other undertaken models, nevertheless FDIA recognition can be quickly done. Further observations suggest that SVM has a higher testing time along with training time than the nonlinear MLP and ARIMA for identifying FDIA effectively. Table 2 shows that the proposed nonlinear LSTM model has the highest time for training and testing to identify FDIA, but showcases the least performance parameters hence signifying a superior attack detection scheme. It can be said that all the models considered in this research for state forecasting and FDIA detection in the smart grid can be easily executed in real-time as their computational efficacy is in the range of μs while the sampling period of SCADA is approximately 100 Hz.

Table 2. Computational efficacy of different models for detecting FDIA.

Models for forecasting	Time for training (μs)	Time for testing (μs)
LSTM	770.34	558.77
MLP [33]	220.35	145.44
SVM [33–36]	480.01	346.02
ARIMA [33–36]	117.22	61.23

5. Conclusion

With large scale sanctioning of IIOT devices within modern power networks, an increasing rate of cyber-attacks has been recently seen which gives rise to highly vulnerable conditions. Thus, the principal focus of the current research is the real-time recognition of FDIA in the smart grid in association with an effectual estimated operating state forecasting. The robust, nonlinear LSTM structure showcases a better horizon to forecast in comparison to the other SOA approaches. Additionally, there is a superior enhancement of the performance metrices for the nonlinear LSTM structure in comparison to MLP, SVM and ARIMA. The proposed nonlinear LSTM model can be successfully executed in real-time since its computational efficacy (i.e. time for testing and training) is in the range of μs which is comparatively lower in comparison to the sampling period of SCADA. In future, the proposed detection strategy can also be implemented under contingency scenarios of the smart grid under a stricter bound over the detection benchmark, which eventually leads to higher possibility of FDIA identification.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data sets are available from the corresponding author on reasonable requests.

Appendix. Proof of Eq. (17)

Proof. To demonstrate the proof of (17), the followings can be inferred from [44]:

$$E\left(t\right)x_1\left(t\right)=\lambda(t)x_1\left(t\right) \tag{A.1}$$

$$x_1\left(t\right)^T E\left(t\right)=\lambda(t)x_1\left(t\right)^T \tag{A.2}$$

where, $\lambda(t)$ represents the eigen value of $E\left(t\right)$ for a particular sampling time t. For an effective normalization of the eigen vectors $x_1\left(t\right)$ and $x_1\left(t\right)^T$, the followings can be inferred:

$$x_1\left(t\right)^T x_1\left(t\right)=1 \tag{A.3}$$

As $E\left(t\right)$ and $E\left(t\right)^T$ have the same eigen values and eigen vectors, hence (A.1) and (A.2) holds. It can be inferred from (A.1), (A.2) and (A.3) that:

$$\lambda\left(t\right)=x_1\left(t\right)^T E\left(t\right)x_1\left(t\right) \tag{A.4}$$

Differentiating both sides with respect to t gives:

$$\frac{d\lambda}{dt}=\frac{dx_1\left(t\right)^T}{dt}E\left(t\right)x_1\left(t\right)+x_1\left(t\right)^T\frac{dE}{dt}x_1\left(t\right)+x_1\left(t\right)^T E(t)\frac{dx_1\left(t\right)}{dt} \tag{A.5}$$

$$=\frac{dx_1\left(t\right)^T}{dt}\lambda\left(t\right)x_1\left(t\right)+x_1\left(t\right)^T\frac{dE}{dt}x_1\left(t\right)+\lambda\left(t\right)x_1\left(t\right)^T\frac{dx_1\left(t\right)}{dt} \tag{A.6}$$

$$=\lambda\left(t\right)\left[\frac{dx_1\left(t\right)^T}{dt}x_1\left(t\right)+x_1\left(t\right)^T\frac{dx_1\left(t\right)}{dt}\right]+x_1\left(t\right)^T\frac{dE}{dt}x_1\left(t\right) \tag{A.7}$$

$$=\lambda\left(t\right)\frac{d}{dt}[x_1\left(t\right)^T x_1\left(t\right)]+x_1\left(t\right)^T\frac{dE}{dt}x_1\left(t\right) \tag{A.8}$$

$$\text{As}\, x_1\left(t\right)^T x_1\left(t\right)=1,\text{hence}:\frac{d\lambda}{dt}=x_1\left(t\right)^T\frac{dE}{dt}x_1\left(t\right) \tag{A.9}$$

This concludes the proof of (17) which shows the rate of change of the eigen values of the error covariance matrix.

References

[1] Abur Ali, Exposito Antonio G. Power system state estimation: Theory and implementation. CRC Press; 2004.

[2] Monticelli A. State estimation in electric power systems: A generalized approach. Springer Science & Business Media; 2012.

[3] Liu Yao, Ning Peng, Reiter Michael K. False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 2011;14(1):1–33.

[4] Kosut Oliver, Jia Liyan, Thomas Robert J, Tong Lang. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In: 2010 First IEEE international conference on smart grid communications. IEEE; 2010, p. 220–5.

[5] Xie Le, Mo Yilin, Sinopoli Bruno. Integrity data attacks in power market operations. IEEE Trans Smart Grid 2011;2(4):659–66.

[6] Hao Jinping, Piechocki Robert J, Kaleshi Dritan, Chin Woon H, Fan Zhong. Sparse malicious false data injection attacks and defense mechanisms in smart grids. IEEE Trans Ind Inf 2015;11(5):1–12.

[7] Boroojeni G, Kianoosh, Hadi Amini M, Iyengar SS. Overview of the security and privacy issues in smart grids. In: Smart grids: Security and privacy issues. Springer; 2017, p. 1–16.

[8] Akhlaghi Shahrokh, Zhou Ning, Huang Zhenyu. Adaptive adjustment of noise covariance in kalman filter for dynamic state estimation. In: 2017 IEEE power & energy society general meeting. IEEE; 2017, p. 1–5.

[9] Guo Yonghe, Ten Chi-Wooi, Jirutitijaroen Panida. Online data validation for distribution operations against cybertampering. IEEE Trans Power Syst 2013;29(2):550–60.

[10] Mehrdad Sarmad, Mousavian Seyedamirabbas, Madraki Golshan, Dvorkin Yury. Cyber-physical resilience of electrical power systems against malicious attacks: A review. Curr Sustain/Renew Energy Rep 2018;5(1):14–22.

[11] Zhang Xialei, Yang Xinyu, Lin Jie, Yu Wei. On false data injection attacks against the dynamic microgrid partition in the smart grid. In: 2015 IEEE international conference on communications. ICC, IEEE; 2015, p. 7222–7.

[12] Sethi Basant Kumar, Mukherjee Debottam, Singh Devender, Misra Rakesh K, Mohanty SR. Smart home energy management system under false data injection attack. Int Trans Electr Energy Syst 2020;30(7):e12411.

[13] Mousavian Seyedamirabbas, Valenzuela Jorge, Wang Jianhui. Real-time data reassurance in electrical power systems based on artificial neural networks. Electr Power Syst Res 2013;96:285–95.

[14] Mohamed S, Amr, Arani Mohammadreza FM, Jahromi Amir A, Kundur Deepa. False data injection attacks against synchronization systems in microgrids. IEEE Trans Smart Grid 2021;12(5):4471–83.

[15] Nikmehr Nima, Moghadam Solmaz M. Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids. IET Cyper-Phys Syst: Theory Appl 2019;4(4):365–73.

[16] Wen Fuxi, Liu Wei. An efficient data-driven false data injection attack in smart grids. In: 2018 IEEE 23rd international conference on digital signal processing. DSP, 2018, p. 1–5.

[17] Kim Jinsub, Tong Lang, Thomas Robert J. Subspace methods for data attack on state estimation: A data driven approach. IEEE Trans Signal Process 2014;63(5):1102–14.

[18] Mukherjee Debottam. Data-driven false data injection attack: A low-rank approach. IEEE Trans Smart Grid 2022;13(3):2479.

[19] Ashfaqur Rahman Md, Mohsenian-Rad Hamed. False data injection attacks with incomplete information against smart power grids. In: 2012 IEEE global communications conference. GLOBECOM, 2012, p. 3153–8.

[20] Liu Xuan, Li Zuyi. False data attacks against ac state estimation with incomplete network information. IEEE Trans Smart Grid 2017;8(5):2239–48.

[21] Li Yuancheng, Wang Yuanyuan. False data injection attacks with incomplete network topology information in smart grid. IEEE Access 2019;7:3656–64.

[22] Ashfaqur Rahman Md, Alam Mohammad. Imperfect nonlinear false data injection attack against largest normalized residual test. In: 2019 IEEE power energy society general meeting. PESGM, 2019, p. 1–5.

[23] Yang Qingyu, Yang Jie, Yu Wei, An Dou, Zhang Nan, Zhao Wei. On false data injection attacks against power system state estimation: Modeling and countermeasures. IEEE Trans Parallel Distrib Syst 2013;25(3):717–29.

[24] Yang Qingyu, An Dou, Min Rui, Yu Wei, Yang Xinyu, Zhao Wei. On optimal PMU placement-based defense against data integrity attacks in smart grid. IEEE Trans Inf Forensics Secur 2017;12(7):1735–50.

[25] Mukherjee Debottam, Sethi Basant K, Chakraborty Samrat, Banerjee Ramashis, Guchhait Pabitra K, Bhunia Joydeep. Real-time mitigation of effects of false data in smart grid: A data diode approach. In: 2021 IEEE 9th region 10 humanitarian technology conference (R10-HTC). 2021, p. 1–6.

[26] Pei Chao, Xiao Yang, Liang Wei, Han Xiaojia. PMU placement protection against coordinated false data injection attacks in smart grid. IEEE Trans Ind Appl 2020;56(4):4381–93.

[27] Zhang Hai Shunjiang Wang, Pei Yujie, Li Yuanyuan, Wang Guangming, Lu Tianqi. Optimal configuration of PMU based on false data injection. In: 2018 international conference on power system technology. POWERCON, 2018, p. 3016–22.

[28] Chaojun Gu, Jirutitijaroen Panida, Motani Mehul. Detecting false data injection attacks in ac state estimation. IEEE Trans Smart Grid 2015;6(5):2476–83.

[29] Drayer Elisabeth, Routtenberg Tirza. Detection of false data injection attacks in power systems with graph fourier transform. In: 2018 IEEE global conference on signal and information processing (GlobalSIP). 2018, p. 890–4.

[30] Drayer Elisabeth, Routtenberg Tirza. Detection of false data injection attacks in smart grids based on graph signal processing. IEEE Syst J 2020;14(2):1886–96.

[31] Bi Suzhi, Zhang Ying J. Graphical methods for defense against false-data injection attacks on power system state estimation. IEEE Trans Smart Grid 2014;5(3):1216–27.

[32] Ashok Aditya, Govindarasu Manimaran, Wang Jianhui. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. Proc IEEE 2017;105(7):1389–407.

[33] Mukherjee Debottam, Chakraborty Samrat, Banerjee Ramashis, Bhunia Joydeep. A novel real-time false data detection strategy for smart grid. In: 2021 IEEE 9th region 10 humanitarian technology conference (R10-HTC). 2021, p. 1–6.

[34] Mukherjee Debottam, Chakraborty Samrat, Banerjee Ramashis, Bhunia Joydeep, Guchhait Pabitra K. A novel deep learning framework to identify false data injection attack in power sector. In: TENCON 2021-2021 IEEE region 10 conference. TENCON, 2021, p. 278–83.

[35] Mukherjee Debottam, Chakraborty Samrat. Real-time identification of false data injection attack in smart grid. In: 2021 IEEE region 10 symposium. TENSYMP, 2021, p. 1–6.

[36] Mukherjee Debottam, Chakraborty Samrat, Banerjee Ramashis, Bhunia Joydeep, Guchhait Pabitra K. Deep learning based real-time detection of false data injection attacks in power grids. In: 2021 22nd international middle east power systems conference. MEPCON, 2021, p. 124–30.

[37] Mukherjee Debottam, Chakraborty Samrat, Ghosh Sandip. Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. Electr Eng 2022;104(1):259–82.

[38] Mukherjee Debottam. A novel strategy for locational detection of false data injection attack. Sustain Energy Grids Netw 2022;31:100702.

[39] Mukherjee Debottam, Chakraborty Samrat, Ghosh Sandip, Mishra Rakesh K. Application of deep learning for power system state forecasting. Int Trans Electr Energy Syst 2021;31(9):e12901.

[40] Mukherjee Debottam, Chakraborty Samrat, Ghosh Sandip. Power system state forecasting using machine learning techniques. Electr Eng 2022;104(1):283–305.

[41] Mukherjee Debottam, Chakraborty Samrat, Guchhait Pabitra K, Bhunia Joydeep. Machine learning based solar power generation forecasting with and without MPPT controller. In: 2020 IEEE 1st international conference for convergence in engineering. ICCE, 2020, p. 44–8.

[42] Mukherjee Debottam, Chakraborty Samrat, Guchhait Pabitra K, Bhunia Joydeep. Application of machine learning for speed and torque prediction of PMS motor in electric vehicles. In: 2020 IEEE 1st international conference for convergence in engineering. ICCE, 2020, p. 129–33.

[43] Mukherjee Debottam, Chakraborty Samrat. A deep learning approach for an effective speed and torque forecasting policy of PMS motors in electric vehicles. In: 2022 second international conference on power, control and computing technologies (ICPC2T). 2022, p. 1–6.

[44] Strang Gilbert. Linear algebra and learning from data. Cambridge: Wellesley-Cambridge Press; 2019.