Deep-Learning-State-Estimation-Aided Detection Framework against False Data Injection Attacks

Bo Liu, Yichen Liu, Xuebo Liu, and Hongyu Wu
The Mike Wiegers Department of Electrical and Computer Engineering
Kansas State University
Manhattan, United States

2024 IEEE Kansas Power and Energy Conference (KPEC) | 979-8-3503-7240-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/KPEC61529.2024.10676057

***Abstract*—False data injection (FDI) attacks can bypass bad data detection and mislead state estimation (SE), resulting in economic losses and security issues. Existing FDI attacks consider the spatial correlation without considering the temporal correlations. Therefore, FDI attacks can correctly mislead the traditional Weighted Least Square SE (WLS-SE) with desired voltage incremental, but hard to accurately mislead the deep-learning-based SE to the desired malicious voltage. This paper first proposes a long-short-term-memory-based state estimator (LSTM-SE), and then proposes a novel deep-learning-SE-aided (DLSEA) attack detection framework. The proposed detection framework utilizes the voltage estimation difference (VED) between the WLS-SE and LSTM-SE to detect the attacks. A fully connected neural network is utilized to classify the VED values for determining either normal system conditions or under cyberattacks. Numerical results in the IEEE 14-bus and IEEE 118-bus systems show the proposed LSTM-SE can approximately estimate the true voltage under FDI attacks, and the proposed detection framework can detect FDI attacks with 0.99 accuracy. We further evaluate the impact of noises on the performance of LSTM-SE and DLSEA.**

***Index Terms*— State estimation, long short-term memory, false data injection attack, deep learning detection.[1]**

I. Introduction

Supervisory control and data acquisition (SCADA) systems monitor the critical infrastructure, including oil pipelines, water distribution and smart grids. However, the IoT and communication techniques cause SCADA systems vulnerable to cyberattacks [1]. The well-known Ukraine blackouts in 2015 and 2016 demonstrate the consequence of cyberattacks on the power system operation, and also show the plausibility of a cyberattack adversary regarding the knowledge and capabilities [2].

False data injection (FDI) attacks are one of cyberattacks designed to mislead the state estimation (SE) function in the control room of smart grids. The FDI attacks manipulate measurements in the SCADA system without being detected by the bad data detector in SE, and therefore cause bias in the estimated voltage [3]. Based on the manipulated voltage, FDI attacks can cause different consequences, such as line overloading, load shedding, unstable system states and even voltage collapse [4]. Different defense mechanisms have been proposed to detect, identify, and mitigate FDI attacks, such as protected sensors [5], phasor measurement unit devices [6], watermarking, meter encoding, and moving target defense methods [7], [8]. However, most of these defense methods require expensive hardware devices.

Machine learning and deep learning (DL) methods have been widely applied to detect FDI attacks, where the cyberattack detection is formulate as a classification problem [9]. Traditional machine learning methods, such as support vector machine [10], Gaussian abnormal detector [11], and multilayer perceptron [12], [13], are used to classify the dimension-reduced normal and compromised measurements. However, the detection accuracy of these machine learning methods is limited.

DL methods can detect FDI attacks with high accuracy rates. In DC power flow model, recurrent neural network (RNN), a sequence classification algorithm, can detect FDI attacks with an accuracy rate of 99% [14]. In AC power flow model, an RNN architecture is used to detect FDI attacks, in which the discrete wavelet transform algorithm is used to extract the hidden time-frequency domain characteristics and features at every specific time [15]. Kaplan et. al. presented a data-driven fault prediction approach and load forecasting approach to conduct fault diagnosis in SGSs, in which the LSTM algorithm is used for feature extraction and fault prediction [16]. However, deep learning algorithms require a long time and large amounts of data for the training process. Liu et al. proposed an FDI attack detection model in which GRU is added to the fully connected layer in convolutional neural networks (CNN) [17]. The CNN-GRU network is designed to train and update network parameters based on historical measurement data of power grid, and extract spatial and temporal characteristics of the data to implement efficient and real-time FDIA detectors. However, the downsides of CNN include a lack of temporal data modeling and long training time [18].

Since the FDI attacks follow the physical laws of the power system, these attacks can mislead the weighted least square state estimation (WLS-SE) to obtain the malicious voltages designed by the attacker. Specifically, the voltage estimated by WLS-SE exactly equals the attacker's malicious voltage target. This is because the traditional SE methods typically utilize the measurements from a single snapshot of the power system without considering the historical measurements. If an SE method learns from both the spatial and temporal relationship of the historical measurements, its estimated voltage under the FDI attacks will not exactly follow the

979-8-3503-7240-3/24/$31.00 ©2024 IEEE

malicious voltage target. Furthermore, the voltage estimated by the learning-based SE method is likely to be closer to true voltage than the attacker's malicious voltage target.

Based on this observation, this paper first proposes a long-short-term-memory-based state estimation (LSTM-SE), which utilizes LSTM to estimate the voltage and the physical power flow model to calculate the loss of the estimated measurements. Then, this paper proposes a novel deep-learning-state-estimation-aided (DLSEA) detection framework to detect FDI attacks, in which a fully connected neural network (FCNN) is used to classify the voltage estimation difference (VED) between the estimated voltage by WLS-SE and that by LSTM-SE. Case studies are conducted in the IEEE 14-bus and 118-bus systems to evaluate the performance of the LSTM-SE, when the system is under attack and free from attacks. We further evaluate the proposed detector in attack detection.

The rest of this paper is organized as follows. In Section II, we provide preliminaries and related work. In Section III, we propose a LSTM-SE method and a novel DLSEA detector. Case studies are conducted in Section IV, and the conclusion is drawn in Section V.

II. Preliminaries

A. AC Weighted Least Square State Estimation

In the power system, the SCADA measurements $\mathbf{z}\in\mathbb{R}^m$ can be expressed by nodal voltage $\mathbf{x}\in\mathbb{R}^n$, i.e., $\mathbf{z}=\mathbf{h}(\mathbf{x})+\mathbf{e}$, where $\mathbf{h}(\cdot)$ is a vector of nonlinear functions and $\mathbf{e}$ is the measurement noise. System operators utilize the state estimation, an important function in the energy management system, to calculate the nodal voltage with the measurements received from the SCADA system. In the AC power flow model, SE is formulated as a weighted least square (WLS) problem, as shown in (1). Gauss-Newton algorithm can be used to solve the WLS problem.

$$\min_{\mathbf{x}} \ (\mathbf{z}-\mathbf{h}(\mathbf{x}))^T\mathbf{K}(\mathbf{z}-\mathbf{h}(\mathbf{x})) \tag{1}$$

where $\mathbf{K}=diag(\sigma_1^{-2},\sigma_2^{-2},...,\sigma_m^{-2})$ is a diagonal matrix of the measurement noise covariance.

B. False Data Injection Attack

The mathematical model of FDI attacks is provided in this subsection. An FDI attack constructs a compromised measurement $\mathbf{z}_a$ by injecting an attack vector $\mathbf{a}$ into the original measurements $\mathbf{z}_0$, i.e., $\mathbf{z}_a=\mathbf{z}_0+\mathbf{a}$. Note that Chi-2 detector is used to detect large measurement errors in the bad data detector of the SE. However, FDI attacks are delicately designed to remain stealthy to Chi-2 detector by following the power flow model of the power system. In the AC power system model, the FDI attack vector $\mathbf{a}$ can be calculated by $\mathbf{a}=\mathbf{h}(\mathbf{x}+\Delta\mathbf{x})-\mathbf{h}(\mathbf{x})$, where $\Delta\mathbf{x}$ is the voltage bias designed by the attacker. In this case, the estimation residual of the FDI attacks is same as that of the original measurement without attacks, and thus the attack is stealthy to BDD [19].

C. LSTM

As a specialized type of RNN, LSTM includes memory cells and gating mechanisms, enabling it to capture and retain long-term dependencies in sequential data. LSTM addresses the vanishing gradient problem of RNN, and thus is widely used for handling sequential data and time series problems. These memory cells are equipped with gating mechanisms that regulate the flow of information, allowing them to selectively remember or forget information at each time step. In an LSTM cell, there are an input gate, a forget gate, an output gate, and a cell state. The input gate $\boldsymbol{i}_t$ controls the flow of new information into the cell, the forget gate $\boldsymbol{h}_t$ determines what information to discard from the cell state, and the output gate $\boldsymbol{o}_t$ regulates the flow of information from the cell to the output of the LSTM [20].

The input of a single LSTM unit is the measurement $\mathbf{z}^t$ at time instant t. $\mathbf{h}^t$ and $\mathbf{h}^{t-1}$ are the hidden vectors at time instant t, and at the last time step t-1, respectively. Compared with RNN, LSTM cell introduces three gates, namely, input gate i, forget gate f, and the output gate o. The mathematical expression of the LSTM cell is given in (2).

$$\begin{aligned}
\Gamma_i &= \sigma(\mathbf{W}_{iz}\mathbf{z}^t+\mathbf{W}_{ih}\mathbf{h}^{t-1}+\mathbf{b}_i)\\
\Gamma_f &= \sigma(\mathbf{W}_{fz}\mathbf{z}^t+\mathbf{W}_{fh}\mathbf{h}^{t-1}+\mathbf{b}_h)\\
\Gamma_o &= \sigma(\mathbf{W}_{oz}\mathbf{z}^t+\mathbf{W}_{oh}\mathbf{h}^{t-1}+\mathbf{b}_o)\\
\tilde{c}^t &= \tanh(\mathbf{W}_{cz}\mathbf{z}^t+\mathbf{W}_{ch}\mathbf{h}^{t-1}+\mathbf{b}_c)\\
c^t &= \Gamma_i\tilde{c}^t+\Gamma_f c^{t-1}\\
\mathbf{y}^t &= \sigma(\mathbf{W}_y\Gamma_o\tanh(c^t)+\mathbf{b}_y)
\end{aligned} \tag{2}$$

where $\mathbf{W}_i,\mathbf{W}_f,\mathbf{W}_o$ are the weights associated with three gates, and $\mathbf{b}_i,\mathbf{b}_f,\mathbf{b}_o$ are the weights associated with three gates.

III. Deep-Learning-State-Estimation-Aided Detection Framework

In this section, we first construct LSTM-SE to estimate the voltage of the power system and then propose a DLSEA detection framework to detect FDI attacks. The relationship between the LSTM-SE (orange section) and the proposed DLSEA detection framework (blue section) is shown in Fig. 1.

The LSTM-SE method is an important part of the proposed DLSEA detection framework. First, the LSTM-SE method is trained using the historical measurements to estimate the voltage of the power system, and then the FCNN in the DLSEA detection framework is trained as a binary classifier using the historical normal measurements and compromised measurements. After the LSTM-SE and the FCNN is well trained, SCADA measurements sampled at each time instant are fed into the proposed DLSEA detection framework to determine whether the measurements are compromised by FDI attacks.

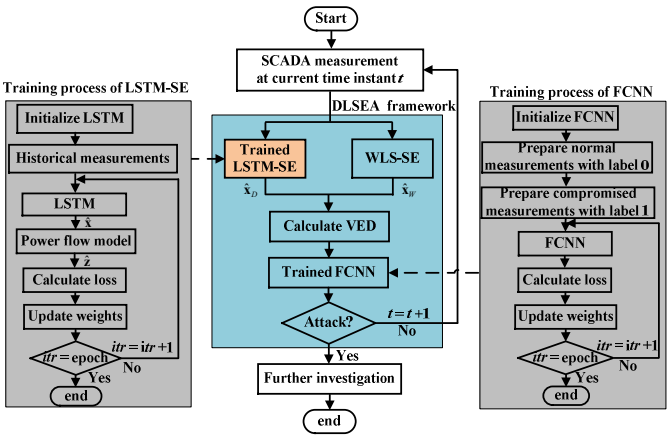


Fig. 1. The relationship between the proposed LSTM-SE and the proposed DLSEA detection framework.

A. LSTM-SE

This subsection proposes an LSTM-based SE method, in which LSTM is applied to learn the voltage state correlations using historical SCADA measurements. The architecture of the proposed LSTM-SE method is shown in Fig. 2. The measurements are fed into the LSTM neural networks, and the output of these networks is system states, i.e., voltage magnitude and angle of all buses. Note that the true voltage states are unknown to the system operator, and thus, the error between the estimated and true states cannot be used as the loss function. The power flow model is utilized to map the estimated states to the estimated SCADA measurements. The physical power flow model can describe the relationship between the power injection and power flow measurement vector $\mathbf{z}=\begin{bmatrix}\mathbf{P}_{in} & \mathbf{Q}_{in} & \mathbf{P}_{f} & \mathbf{Q}_{f}\end{bmatrix}$ and system state $\mathbf{x}=\begin{bmatrix}\mathbf{v} & \boldsymbol{\theta}\end{bmatrix}$, as follows:

$$\begin{aligned} P_{in}^{i} &= \sum_{j=N(i)} V_i V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \\ Q_{in}^{i} &= \sum_{j=N(i)} V_i V_j (G_{ij}\sin\theta_{ij} + B_{ij}\cos\theta_{ij}) \\ P_{f}^{ij} &= -V_i^2 G_{ij} + V_i V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \\ Q_{f}^{ij} &= -V_i^2 B_{ij} + V_i V_j (G_{ij}\cos\theta_{ij} - B_{ij}\sin\theta_{ij}) \end{aligned} \tag{3}$$

where P_{in}^{i} and Q_{in}^{i} are active and reactive power injection of Bus i, respectively, and P_{f}^{ij} and Q_{f}^{ij} are active and reactive power flow of transmission line between Bus i and Bus j; G_{ij} and B_{ij} are the real and imaginary part of the admittance matrix, respectively; V_i is the voltage magnitude of Bus i; θ_{ij} is the voltage angle difference between Bus i and Bus j; and N(i) is the set of neighbor buses of Bus i.

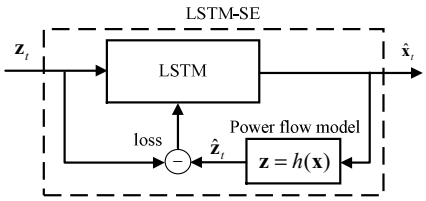


Fig. 2. The framework of LSTM-SE.

For the loss function, we select cumulative mean square error (MSE) between the actual measurements $\mathbf{z}$ and estimated measurements $\hat{\mathbf{z}}$, i.e., $L_0=\frac{1}{m}\sum_t (z_t-\hat{z}_t)^T(z_t-\hat{z}_t)$, where $\hat{\mathbf{z}}$ is calculated by the estimated states $\hat{\mathbf{x}}$ based on the power flow model (3). Then, we can update the weights and biases of the LSTM using back-propagation.

B. DLSEA Detection Framework

In this section, we propose a novel DLSEA attack detection framework that learns and classifies the voltage estimation differences between the attacker's malicious voltage and the voltage estimated by the deep-learning state estimator. The deep-learning attack detection framework is shown in Fig. 3. It is assumed that the attacker maliciously injects FDI attacks $\mathbf{a}_t$ into the SCADA measurements $\mathbf{z}_t$ at the current time instant t. When the SCADA system receives the latest measurements (compromised measurement $\mathbf{z}_a^t$), the system operator can apply the proposed attack detection framework to determine whether the system is under attack. The detection framework applies both WLS-SE and LSTM-SE to estimate the voltage. Then, a fully connected neural network is used to classify the voltage estimation difference.

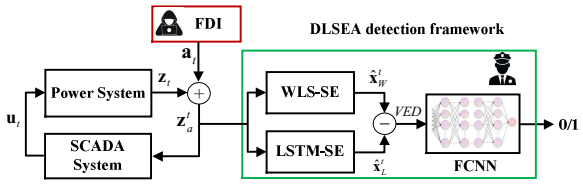


Fig. 3. The DLSEA attack detection framework.

The deep-learning attack detection framework is designed based on three observations. First, the attacker's malicious voltage generally is not consistent with the temporal correlation of historical voltage states. Second, the estimated voltage by the LSTM-SE follows the temporal correlation of historical voltage states, and thus will not exactly equal the attacker's malicious voltage. Third, the attacker's malicious voltage is unknown to the defender (system operator). However, the traditional widely-used power system state estimation method, i.e., WLS-SE, is vulnerable to FDI attacks. Consequently, the estimated voltage by the WLS-SE is considered to be equal to the attacker's malicious voltage. Therefore, the VED can be selected as the feature for an attack detection classifier. The VED between the attacker's malicious voltage and the voltage estimated by the LSTM-SE is approximated by the VED between WLS-SE and LSTM-SE, defined as follows:

$$VED = \hat{\mathbf{x}}_W - \hat{\mathbf{x}}_L \tag{4}$$

where $\hat{\mathbf{x}}_W$ is the estimated voltage from WLS-SE and $\hat{\mathbf{x}}_L$ is the estimated voltage from LSTM-SE.

Then, an FCNN is constructed as a binary attack detection classifier. The input lay has 2n-1 neurons (the number of voltage states), and the output lay has one neuron. The width and depth of the network is adjusted by the complexity of the power system. The structure of FCNN for the IEEE 14-bus and 118-bus systems is shown in Table I, where l_k denotes the number of neurons in the k-th hidden layer. For the hidden layers, the rectified linear unit (ReLU) is selected as the activation function since it can introduce the property of non-linearity to a deep learning model and solve the vanishing gradients issue. We adopt the sigmoid activation function for the output layer, and thus, the activation function can map the hidden layer output into the probability of the attack detection.

Table I. The structure of fully connected neural network

System	States	k	l_k
14	27	5	{100,200,400,200,100}
118	235	6	{100,200,400,400,200,100}

IV. Case Study

We first evaluate the performance of LSTM-SE method in estimating the voltage and then assess the performance of the proposed detection framework in detecting FDI attacks. In SE, there are 68 and 400 measurements in the IEEE 14-bus and 118-bus systems, respectively. In the case study, we have five measurement type, including active power flow, reactive power flow, active power injection, active power injection and voltage magnitude. In each measurement, we adopt zero-mean Gaussian distributed noise, that has a standard deviation as 1% of the actual measurement. We train the LSTM-SE model with different network structures, and then select the structure with

the best performance based on cross-validation. The algorithms are performed on a computer with an Intel Core i9-13900 CPU and a Nvidia RTX 4090 24GB GPU.

The historical measurements and voltage are generated using the one-year load profile of ERCOT Utility in the IEEE 14-bus system, and the one-year load profile of WECC in the IEEE 118-bus system [21], [22]. 80% of the data is used as the training data, and the remaining data is used as the testing data for the LSTM-SE. The testing data for the LSTM-SE method is further used as the normal measurements for the DLSEA detection framework. Then, FDI attacks are launched on each normal measurement vector. There are 3500 and 5000 FDI attacks as the compromised measurements in the IEEE 14-bus and 118-bus systems, respectively.

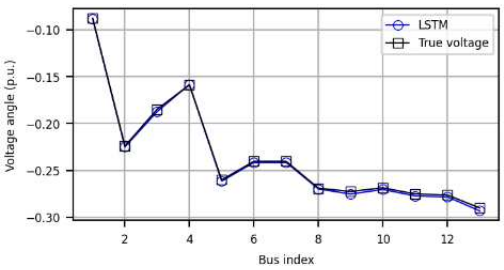
In each FDI attack, the voltage angles of one randomly selected bus are compromised. The normal and compromised data are divided into the DLSEA detection framework's training and testing data. For the DLSEA detector, the precision and the F1 score are used to measure its performance in detecting FDI attacks.

We employed the Adam optimizer, recognized as one of the most effective optimization algorithms, to optimize both LSTM-SE and DLSEA models. Adam's adaptive learning rates and momentum help expedite convergence and enhance model performance across various tasks. We conduct random search to determine the constant learning rates, batch size, and model architecture based on the performance of the model. Since LSTM-SE and FCNN classifier are both pre-trained offline, the proposed DLSEA framework can achieve good execution time. In the IEEE 118-bus system, the execution time of LSTM-SE and FCNN is less than 2ms

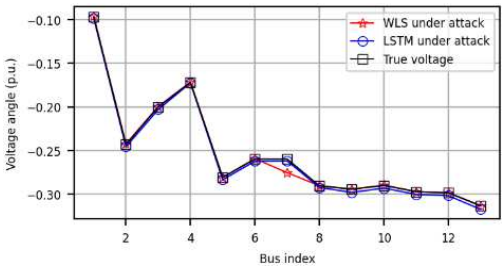
A. Performance of LSTM-SE

In this section, we evaluate the accuracy of the voltage estimation of LSTM-SE. The performance of LSTM-SE is measured in quantity by the root mean square error (RMSE), formulated as $RMSE = \sqrt{\sum_{i=1}^{n} \frac{(x_i^0 - \hat{x}_i)^2}{n}}$, where x_i^0 and $\hat{x}_i$ are the actual and estimated value of the i-th state, respectively.

We first demonstrate the voltage estimated by the LSTM-SE under no attack and under attack conditions, respectively. Under no attack conditions, the LSTM-SE's estimated voltage angle at 352 Day 12 AM is shown in Fig. 4(a). It is seen that the LSTM-SE's estimated voltage angle is almost the same as the true voltage value. In Fig. 4(b), an FDI attack decreases the voltage angle of Bus 7. It is seen that WLS-SE is vulnerable to FDI attacks following the attack's target. However, LSTM-SE is robust to the FDI attacks, and its estimation is closer to the true voltage of Bus 7. The estimation accuracy of LSTM-SE under FDI attacks can contribute to the effectiveness of the proposed detection framework.



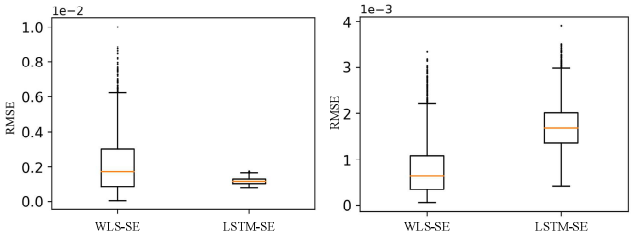
(a) Voltage angle estimation under no attack



(b) Voltage angle estimation under attacks

Fig. 4. The voltage estimation of LSTM-SE under no attack and attack conditions.

Then, we compare the RMSE of LSTM-SE with that of the traditional WLS-SE using measurements from the testing dataset consisting of 3500-time instants. In Fig. 5(a), we can see that the whiskers in LSTM-SE's RMSE are similar to the median of WLS-SE's RMSE in voltage magnitude estimation. The LSTM-SE outperforms the WLS-SE in voltage magnitude estimation, but it performs slightly worse in the angle estimation compared with WLS-SE. This is because the voltage magnitudes of some buses are directly measured and the angle of all buses is not measured.



(a) Voltage magnitude (b) Voltage angle

Fig. 5. Boxplot of RMSE in WLS-SE and LSTM-SE.

B. Performance of DLSEA Detection Framework

We evaluate the performance of the proposed DLSEA detection framework in detecting FDI attacks in the IEEE 14-bus and 118-bus systems. Historical measurements of 3500 and 5000 are labeled as normal measurements in the IEEE 14-bus and 118-bus systems, respectively. Then, we generate one FDI attack on each measurement vector, labeled as the compromised measurements. In each FDI attack, the voltage angles of one randomly selected bus are compromised, and their incremental values are randomly selected according to the uniform distribution $\Delta\theta = U(0.08\bar{\theta}_1, 0.12\bar{\theta}_1)$, where $\bar{\theta}_1$ is the average voltage angle at time instant 1. Thus, 10000 normal and compromised measurement vectors are divided into the training and testing data for the DLSEA detection framework in the IEEE 118-bus system and 7000 in the IEEE 14-bus system.

We conduct 5-fold cross-validation in the dataset of normal and compromised measurements. The average precision, accuracy, and F1 score in 5-fold cross-validation are shown in Table II. It is seen that the proposed detection framework can effectively detect FDI attacks with extremely low false positive and false negative rates.

Table II. The performance of DLSEA detection framework.

System	Precision	Accuracy	F1 score
14-bus	0.999	0.997	0.997
118-bus	1.000	0.999	0.999

We evaluate the performance of LSTM-SE and DLSEA under three different Gaussian noise standard deviations (1%, 2%, and 3% of the actual measurement) in the IEEE 14-bus

system. The performance of DLSEA detection is shown in Table III. With a larger noise, the precision of DLSEA decreases. When there exists 3% standard deviation, the precision of DLSEA is 95.1%.

Table III. The performance of DLSEA framework under different noises.

Noise	Precision	Accuracy	F1 score
0.01	0.999	0.997	0.997
0.02	0.989	0.994	0.994
0.03	0.951	0.973	0.973

V. Conclusions

Based on the recurrent network's learning capability of sequential data, this paper first applies LSTM networks to construct LSTM-SE. We evaluate the performance of LSTM-SE in the IEEE 14-bus system. The LSTM-SE outperforms the traditional WLS-SE in voltage magnitude estimation with an RMSE value lower than 0.002, but it performs slightly worse in the angle estimation compared with the WLS-SE with an RMSE value lower than 0.004. This paper found that the VED of each state is close to zero in normal conditions, and the VED of the attacked state becomes non-zero under FDI attacks. Based on the characteristics of the VED, this paper proposes a novel DLSEA detection framework to detect FDI attacks against power system statics state estimation, in which an FCNN is used to classify the VED as a binary classification problem. In case studies, 5-fold cross-validation is conducted on the normal and compromised measurement dataset in the IEEE 14-bus and 118-bus systems. Simulation results verify that the proposed DLSEA detection framework can effectively detect FDI attacks with 0.999 precision. In future work, the proposed detection framework will be applied to the localization and data recovery of FDI attacks on power systems.

Acknowledgment

This material is based upon work supported by the U.S. National Science Foundation under Grant No. 1929147 and No. 2146156, and by the United States Office of Naval Research under grant N00014-23-1-2777.

References

[1] F. Mercaldo, F. Martinelli, and A. Santone, "Real-Time SCADA Attack Detection by Means of Formal Methods," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Jun. 2019, pp. 231–236.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[3] B. Liu, H. Wu, Q. Yang, H. Zhang, Y. Liu and Y. Zhang, "Matrix-Completion-Based False Data Injection Attacks Against Machine Learning Detectors," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 2146-2163.

[4] H. Zhang, B. Liu, and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[5] S. Bi and Y. J. Zhang, "Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[6] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU Placement Protection Against Coordinated False Data Injection Attacks in Smart Grid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4381–4393, Jul. 2020.

[7] B. Liu and H. Wu, "Optimal D-FACTS Placement in Moving Target Defense against False Data Injection Attacks," *IEEE Trans. Smart Grid*, pp. 1–1, 2020.

[8] B. Liu, H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu, "Hidden Moving Target Defense against False Data Injection in Distribution Network Reconfiguration," in *2018 IEEE Power Energy Society General Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[9] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717-729, March 2014.

[10] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine Learning Methods for Attack Detection in the Smart Grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[11] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[12] M. Ashrafuzzaman *et al.*, "Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Jun. 2018, pp. 219–225.

[13] 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-Phys. Syst. Theory Appl.*, vol. 2, no. 4, pp. 161–171, 2017.

[14] A. Ayad, H. E. Z. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using Recurrent Neural Networks," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb. 2018, pp. 1–5.

[15] J. J. Q. Yu, Y. Hou and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271-3280, July 2018.

[16] H. Kaplan, K. Tehrani, and M. Jamshidi, "Fault Diagnosis of Smart Grids Based on Deep Learning Approach," in *2021 World Automation Congress (WAC)*, Aug. 2021, pp. 164–169.

[17] M. Lu, L. Wang, Z. Cao, Y. Zhao, and X. Sui, "False data injection attacks detection on power systems with convolutional neural network," *J. Phys. Conf. Ser.*, vol. 1633, no. 1, p. 012134, Sep. 2020.

[18] E. Balouji and O. Salor, "Classification of power quality events using deep learning on event images," *2017 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA)*, Shahrekord, Iran, 2017, pp. 216-221.

[19] G. Hug and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[20] A. Shewalkar, D. Nyavanandi, and S. A. Ludwig, "Performance Evaluation of Deep Neural Networks Applied to Speech Recognition: RNN, LSTM and GRU," *J. Artif. Intell. Soft Comput. Res.*, vol. 9, no. 4, pp. 235–245, Sep. 2019.

[21] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[22] "Electric Reliability Council of Texas." Accessed: Jun. 16, 2022. [Online]. Available: https://www.ercot.com/