Establishing a detection model data attacks in power distribution system

Sihang Yu[1,*], Zhaoxiang Li[1], Wenbin Lin[1], Wujie Chao[1], Jiansheng Guo[1], Jie Jia[1], Zhigeng Zhang[1]

[1]State Grid Fujian Electric Power Research Institute, Fuzhou, China 350007

Abstract. The safe operation of smart distribution network is highly dependent on the powerful technical guarantee provided by the function of information link, which makes the network vulnerable to the threat of malicious data injection and other network attacks during the operation. In order to ensure that this kind of malicious data injection attack can be detected sensitively in the operation of power grid, this paper proposes a kind of power system state estimation malicious data attack defense model based on historical data. Firstly, the Long Short-Term Memory(LSTM) network is trained with the historical state quantity to realize the state prediction model. The prediction results are used as a reference, and the deviation between the prediction and the real-time estimate is calculated to break the concealment of malicious data. Simulation results of IEEE33-bus power system verify the accuracy of prediction and the effectiveness of the proposed method for online detection of hidden malicious data.

1 Introduction

With the construction of power grid automation system, reliable sensor network and its deep integration with ubiquitous information network and energy network, the traditional power grid is gradually transformed into a smart grid with wide cooperation between information system and physical system and autonomous behavior ability. Because of the complexity and openness of smart grid system, the risk of network attack on power grid is intensified. For example, in 2016, the Ukrainian State Ministry of Electricity was attacked by hackers, causing a massive blackout in the country. Therefore, the research of smart grid attack detection is of great significance.

Liu Y. et al proposed the malicious data attack [1] for the first time in 2009, which made use of the loophole in the traditional bad data detection mechanism of the control center to induce the state estimation of the control center to produce a wrong estimation of the system state, thus causing the control center to give wrong instructions and thus affecting the operation of the power grid. With the deepening of research, good progress has been made in accomplishing malicious data injection attacks with less or completely unknown system topology and line parameter information [2]. At present, there are three kinds of malicious data attacks: state attack, topology attack and load distribution attack. Among them, state attack is the easiest and most common attack, so this paper analyzes the state attack in malicious data attack, and establishes a set of methods that can effectively detect this type of attack.

Literature [3] adopted the graph theory method to select a group of protected quantity measurements to curb the generation of malicious data. Although PMU can reduce the risk of malicious data attack through encryption technology, it does not mean that it can be completely trusted. Once the encryption algorithm is broken, it will bring greater harm to the operation of the power grid. Moreover, the high investment cost limits the application of measurement protection method. The introduction of artificial intelligence technology provides a new idea for the study of malicious data injection attack detection. Artificial intelligence can identify the attack events through continuous learning. In Literature [4], the attack events were first labeled, and the semi-supervised learning method was introduced to determine the optimal detection threshold based on the tag data; Literature [5] used conditional Gauss-Bernoulli constrained Boltzmann machine as a classifier to analyze the time attack mode provided by real-time measurement data from instruments with different geographical distribution, and to carry out secondary screening of attack data missed by traditional residual detection method. In this paper, considering the time connection between the data due to the inertia and momentum of the system, the LSTM network is used to predict the future running state of the power system, and the prediction information is used as a reference. The deviation data between the Euclidean distance prediction information and the real-time estimation state change is described to detect malicious attacks.

* Corresponding author: yu_sihang@fj.sgcc.com.cn

2 Principle of malicious data attack in power system

The relationship between measurement value and state estimation is as follows:

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

Where, z is the assumed measurement truth value, it is m dimension vector; $h(x)$ is the measurement function representing the numerical relationship between measurement and state quantity; x is state quantity to be estimated, v_z is the measurement error vector. The estimated state quantity is obtained by the weighted least square method, as shown in Equation:

$$\hat{x} = \arg\min_x (z + \Delta L - h(x))^{\mathrm{T}} W (z + \Delta L - h(x)) \tag{2}$$

After iteration of Gauss-Newton iterative method, the following results can be obtained:

$$\Delta\hat{x}^{(l)} = [H^T(\hat{x}^{(l)}) R^{-1} H(\hat{x}^{(l)}))]^{-1} H^T(\hat{x}^{(l)}) R^{-1}[z - h(\hat{x}^{(l)})] \tag{3}$$

$\Delta\hat{x}^{(l)}$ is the iteration difference, and if it is less than the threshold, it indicates the iteration convergence. The traditional detection method based on residual bad data is the maximum standardized residual method, which is expressed as:

$$r = z - h(\hat{x}) \tag{4}$$

When the $\|r\|$ value is greater than the threshold value, it indicates that there is bad data in the quantity measurement. When the attacker injects the false data vector and superimposes it on the original measurement data, the measurement data becomes $z_{\text{bad}} = z + a$; The state estimation result will be affected by it and the estimated value will deviate from the original value to $x_{\text{bad}} = \hat{x} + c$, $c = [c_1, c_2, ..., c_n]^{\mathrm{T}}$ represents a state offset. Substitute it into Equation (4), and the residual expression becomes as follows:

$$\|r\| = \|z_{\text{bad}} - H\hat{x}_{\text{bad}}\| = \|z + a - H(\hat{x} + c)\| = \|z - H\hat{x} + a - Hc\| \tag{5}$$

Obviously, when $a = Hc$, the following formula holds:

$$\|r\| = \|z_{\text{bad}} - Hx_{\text{bad}}\| = \|z - H\hat{x}\| < \tau \tag{6}$$

Therefore, as long as the injected false data is satisfied $a = Hc$, largest normalized residual detection will not detect this attack. The attacker takes advantage of this point. After cracking the encryption of the communication system, he first uses principal component analysis method to obtain the elements in the measurement matrix H , and then constructs false data and superimposes it on the original measurement data to achieve the purpose of maliciously tampering with the measurement value. In turn, the state estimation is affected, which leads to the wrong information received by the control center and leads to wrong decisions.

3 Detection system modeling

In this paper, the establishment process of power system state estimation malicious data attack defense system is divided into three parts: firstly, the online prediction part uses the historical data to train the optimal LSTM prediction model. And then carries on the state prediction to get the state prediction value at the current moment. Finally, the change of the deviation between the predicted value and the real-time estimate value is used to detect the malicious data attack.

3.1 State prediction based on LSTM

The historical data of distribution network mainly includes operation information and measurement information, which contains the spatiotemporal correlation between the operation states of distribution network [6]. In this paper, the state information of time series with certain correlation is taken as the whole for historical data modeling. LSTM is an improved model of RNN (recurrent neural network) and can select the timing information. Figure 1 shows the LTSM sequence structure diagram [7]. $x(t)$ is input at time t ; $c(t)$ is memory state at time t and stores long-term memories. $h(t)$ is output at time t .

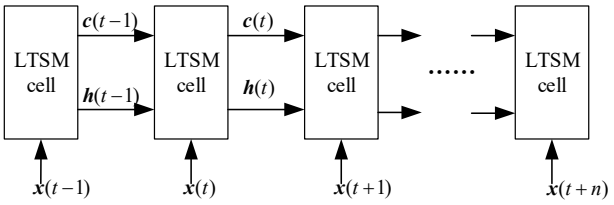

Fig. 1. LTSM Sequential logic framework .

Figure 2 shows the LSTM model architecture. Forget gate, input gate and output gate control the input of information.

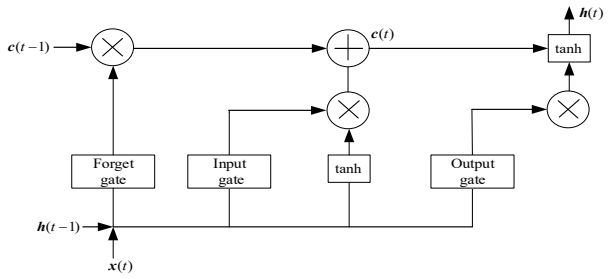

Fig. 2. Unfolded structure of LSTM network .

Firstly, the forgetting gate is used to choose whether there are some long-term features that need to be forgotten. The calculation formula is as follows:

$$f_t = \sigma\left(W_f \left[h_{t-1}, x_t\right] + b_f\right) \tag{7}$$

Where W_f is the weight matrix for forget gate; b_f is the bias for forget gate; h_{t-1} and x_t constitute input vectors $\left[h_{t-1}, x_t\right]$ for forget gate. f_t outputs a number between 0 and 1. If 0, it indicates that the feature has been forgotten from long-term memory, but if 1, it indicates that the feature has been retained. σ is activation function:

$$\sigma(x)=\frac{1}{1+\mathrm{e}^{-x}} \tag{8}$$

Input gate:

$$\boldsymbol{i}_t=\sigma\left(\boldsymbol{W}_i\left[\boldsymbol{h}_{t-1},\boldsymbol{x}_t\right]+\boldsymbol{b}_i\right) \tag{9}$$

Where $\boldsymbol{W}_i$ is the weight matrix for input gate; $\boldsymbol{b}_i$ is the bias for input gate. The control through the input gate can discard the current unimportant information.

Cell:

$$\tilde{\boldsymbol{c}}_t=\tanh\left(\boldsymbol{W}_c\left[\boldsymbol{h}_{t-1},\boldsymbol{x}_t\right]+\boldsymbol{b}_c\right) \tag{10}$$

$$\boldsymbol{c}_t=\boldsymbol{f}_t\odot\boldsymbol{c}_{t-1}+\boldsymbol{i}_t\odot\tilde{\boldsymbol{c}}_t \tag{11}$$

Where $\boldsymbol{W}_c$ is the weight matrix for state; $\boldsymbol{b}_c$ is the bias for state. $\tilde{\boldsymbol{c}}_t$ is memory state for cell at time t. $\tilde{\boldsymbol{c}}_t$ and $\boldsymbol{c}_{t-1}$ form the new input sate $\boldsymbol{c}_t$; tanh is activation function:

$$\tanh(x)=\frac{\mathrm{e}^{x}-\mathrm{e}^{-x}}{\mathrm{e}^{x}+\mathrm{e}^{-x}} \tag{12}$$

Output gate:

$$\boldsymbol{o}_t=\sigma\left(\boldsymbol{W}_o\left[\boldsymbol{h}_{t-1},\boldsymbol{x}_t\right]+\boldsymbol{b}_o\right) \tag{13}$$

$$\boldsymbol{h}_t=\boldsymbol{o}_t\odot\tanh\left(\boldsymbol{c}_t\right) \tag{14}$$

Where $\boldsymbol{W}_o$ is the weight matrix for output gate; $\boldsymbol{b}_o$ is the bias for output gate; $\boldsymbol{o}_t$ and $\boldsymbol{c}_t$ Jointly determine the output $\boldsymbol{h}_t$ at moment t.

3.2 Identification of attack

When the system is under malicious attack, the measurement value of malicious change will make the result of state estimation jump to the method expected by the attacker [8]. At this time, the deviation between the predicted result and the actual estimated result will gradually become larger. In order to extract the numerical information of the deviation between the predicted value and the estimated value better, the Euclidean distance are selected as the numerical monitoring indexes. The Euclidean distance describes the degree of dissimilarity between two samples by calculating the true distance of the dimensional sample sequence between two points. The expression is as follows:

$$\mathrm{d}_k=[\sum_{i=1}^{n}(x_{k,i}^{\mathrm{L}}-x_{k,i}^{\mathrm{Y}})]^{1/2} \tag{15}$$

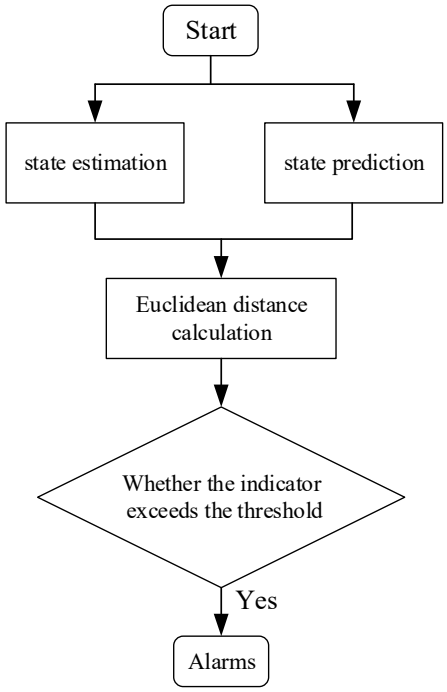

Fig. 3. Flow chart of online detection against malicious data

4 Calculation example and result analysis

4.1 The simulation setup

In this paper, IEEE33 bus distribution system is selected as an example for analysis. The original load data is from the data published by the New York Electric Power Authority, and the load data of IEEE33 bus are constructed by using the data. The sampling interval is 36s, and 100 points will be collected in an hour.

12,000 historical status values were used to train the LTSM model, and 2400 data were predicted for the following day, and the model was continuously updated and corrected through real-time operation data.

The reliability of the prediction results directly affects the effectiveness of the defense means, and a more accurate state prediction method can guarantee a higher prediction confidence, which is helpful to improve the detection rate of malignant data. This experiment verifies the effectiveness of the prediction method proposed in this paper. The mean error and standard deviation of some nodes are shown in the table:

Tab 1. Absolute error of amplitude prediction of some nodes in the IEEE 33-bus

BUS	The mean of the absolute error mean （10-4/pu）	The standard deviation of the absolute mean of error
3	0.7749	0.59057
7	1.5815	1.1765
15	1.5873	1.2060
18	2.5243	1.9231
21	1.1166	0.8535
25	3.1455	2.4042
33	4.9654	0.5906

Tab 2. Absolute error of phase Angle prediction of some nodes in the IEEE 33-bus system

BUS	The mean of the absolute error mean（10-4/rad）	The standard deviation of the absolute mean of error
3	0.64134	0.4900
7	0.31213	0.2259
15	0.54877	0.4231
18	2.0831	1.6125
21	1.1071	0.8506
25	3.0382	2.3281
33	3.8267	2.9340

In order to make malicious data attack concealment enough, the attack mode simulated in this paper will make the offset of state quantity fluctuate within the range of 1% to 10% of the original value. 100 times of malicious data of varying intensity will be continuously carried out in the test samples. The state changes are shown in Figure 5-7:

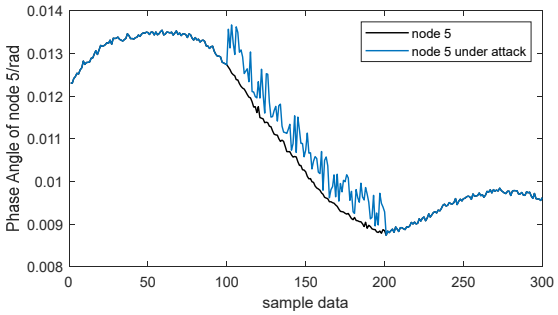

Fig.4. Changes of state quantity before and after attack

The normal and attacked detection values obtained by Euclidian distance detector are shown in Fig. 5 and Fig. 6 respectively. According to the comparative analysis, under normal circumstances, the detection value d(k) obtained by the Euclidian distance detector is basically stable within a certain range. When the system is attacked, the detection value d(k) is significantly higher than that under normal conditions.

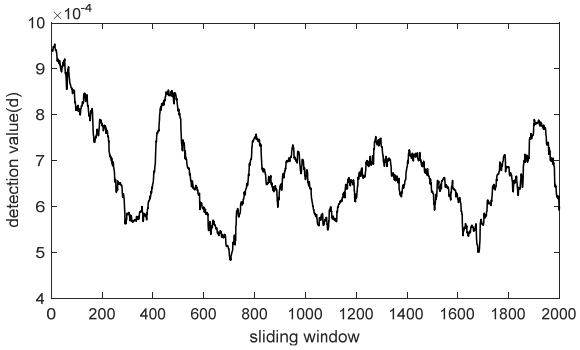

Fig. 5. Euclidean distance changes under normal conditions

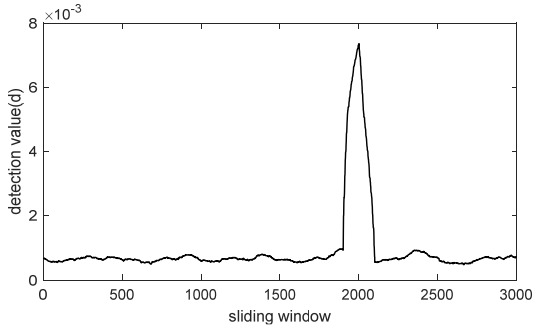

Fig. 6. The Euclidean distance variation after an attack over a period of time

4.2 Choice of optimal threshold

When the detection value exceeds the threshold value, the detector triggers an alarm signal. False alarm rate indicates the probability of detector alarm due to normal state fluctuation. Missed detection rate refers to the probability that the detector fails to alarm when attacked, and the calculation expression is as follows:

$$FAR = \frac{FN}{FN + TN} \tag{16}$$

$$MAR = \frac{FP}{TP + FP} \tag{17}$$

Where, FN represents the number of normal data identified as an alarm, and TN represents the number of normal data not triggering the detector alarm; TP represents the number of successful alarms after being attacked, and FP represents the number of failed alarms after successful attacks. As the enlargement of Euclidean distance is a cumulative process, there will be a certain lag in the detection and alarm time. In order to ensure the sensitivity of detection, the alarm within 15 sliding Windows will be called a successful detection.

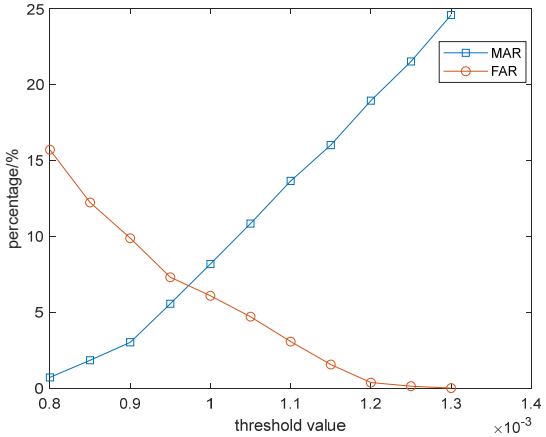

Fig. 7. The false alarm rate and the missed alarm rate curve

According to the figure 7, with the increase of the threshold, the false alarm rate of the detector gradually decreases, while the false alarm rate gradually increases. The increase of the false alarm rate is smaller than the decrease of the false alarm rate. The corresponding value when the equal error rate is 6.75% is selected as the threshold value of the detector.

5 Conclusion

In this paper, the detection problem of fraudulent data attacks in distribution network state estimation is studied. First, the state is predicted in advance by using the long and short memory network, and the Euclidean distance is used as the index to judge the consistency between the predicted state and the real-time estimated state. According to the change of the index value, it is judged whether malicious data attack is suffered. The validity of the proposed method is verified by experiments. In future work, with the update of attack mode and means, it is necessary to continue to explore more effective, more intelligent and more generalized detection methods on the basis of existing detection algorithms to enhance the detection ability of detectors against different types of FDIA.

References

1. Liu Yao，Ning Peng，Reiter M K．False data injection attacks against state estima-tion in electric power grids[C]//Proceedings of the 16th ACM conference on Computer and communications security．New York：ACM，2009：21-32．
2. Chin W L，Lee C H，Jiang T．Blind false data attacks against AC state estimation based on geometric approach in smart grid communications[J]. IEEE Transactions on Smart Grid，2017：6298-6306
3. Bi S, Zhang Y J. Graphical Methods for Defense Against False-Data injection Attacks on power system state estimation[J]. IEEE Transactions on Smart Grid, 2014, 5(3): 1216-1227
4. FOROUTANS, A, SALMASIF, R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method[J]. IET Cyber-Physical Systems: Theory& Applications,2017,2(4): 161-171.
5. HE Youbiao, MENDIS G J, WEI Jin. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2505-2516.
6. YU J J Q, Hou Yunhe, Li V O K. Online false data injection attack detection with wavelet transform and deep neural net works[j].IEEE Transactions on Industrail Informatics, 2018, 14(7): 3271-3280.
7. Graves A. Long short-term memory[M]. Supervised Sequence Labeling with Re-current Neural Networks. Textbook, Studies in cmputational Intelligence, Springer, 2012.
8. Qi J J, Sun K, Wang J H, Liu H. Dynamic State Estimation for Multi-Machine Power System by Unscented Kalman Filter With Enhanced Numerical Stability. IEEE Transac-tions on smart grid 2018, 9(2): 1184-1196